PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-112824
(43)Date of publication of application : 21.04.2000

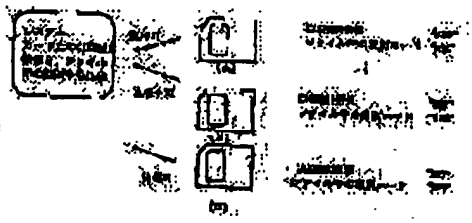
(51)Int.Cl. G06F 12/14
G06F 12/06
G11C 16/02

(21)Application number : 10-282527
(22)Date of filing : 05.10.1998

(71)Applicant : TOSHIBA CORP
(72)Inventor : TANAKA YOSHIYUKI
SUKEGAWA HIROSHI
NAKABAYASHI MIKITO
NAKAMURA HIROSHI

(54) MEMORY SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a memory system capable of securing the protection of copyright at the time of using a flash memory card or the like.
SOLUTION: In the memory system using detachable storage media A-C and data stored in these media A-C, individual information for individually identifying each storage medium is stored in the storage medium, and in the case of utilizing data stored in the storage medium, the individual information of the storage medium is required. Individual information for individually identifying each of storage media A-C is stored in the storage medium, information related to each individual information is stored in data stored in each storage medium, and in the case of utilizing the data stored in the storage medium, coincidence between the individual information stored in the storage medium and the relative information in the data is checked and then the use of the data in the system is permitted.



LEGAL STATUS

[Date of request for examination] 07.10.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－112824
（P2000－112824A）
(43)公開日　平成12年４月21日(2000.4.21)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
G06F	12/14	320	G06F	12/14	320C 5B017
	12/06	515		12/06	515H 5B025
G11C	16/02		G11C	17/00	601E 5B060

審査請求　未請求　請求項の数５　ＯＬ　（全 22 頁）

(21)出願番号　特願平10－282527

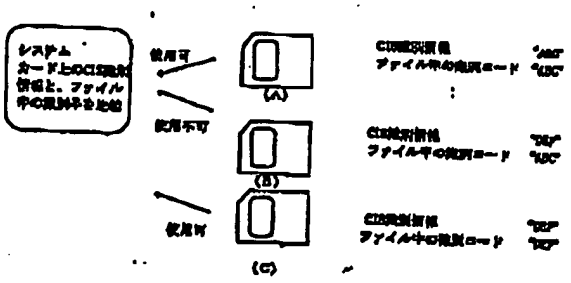
(22)出願日　平成10年10月５日(1998.10.5)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　田中　義幸
神奈川県川崎市幸区堀川町580番１号　株式会社東芝半導体システム技術センター内
(72)発明者　助川　博
神奈川県川崎市幸区堀川町580番１号　株式会社東芝半導体システム技術センター内
(74)代理人　100083161
弁理士　外川　英明

最終頁に続く

(54)【発明の名称】　メモリシステム

(57)【要約】
【課題】　フラッシュメモリカード等の利用に際し、著作権の保護が確保されるメモリシステムを提供する。
【解決手段】　着脱可能な記憶媒体と前記記憶媒体中に格納されたデータを使用するメモリシステムにおいて、前記記憶媒体には前記記憶媒体を個別に識別するための個別情報が保持され、前記記憶媒体中に格納されるデータを使用する際は、前記記憶媒体の個別情報を必要とすることを特徴とするメモリシステム。



1

【特許請求の範囲】

【請求項１】　着脱可能な記憶媒体と、前記記憶媒体中に格納されたデータを使用するメモリシステムにおいて、

前記記憶媒体には、前記記憶媒体を個別に識別するための個別情報が保持され、前記記憶媒体中に格納されるデータを使用する際は、前記記憶媒体の個別情報を必要とすることを特徴とするメモリシステム。

【請求項２】　着脱可能な記憶媒体と、前記記憶媒体中に格納されたデータを使用するシステムにおいて、

前記記憶媒体には、前記記憶媒体を個別に識別するための個別情報が保持され、前記記憶媒体中に格納されるデータには上記個別情報に関連付けられた情報が格納され、前記記憶媒体中に格納されるデータを使用する際は、前記記憶媒体の個別情報と前記データ中の関連付けられた情報の合致を確認後、前記システム中での前記データの使用を許可することを特徴とするメモリシステム。

【請求項３】　前記個別情報の読み出しは、記憶媒体内のデータの読み出しと異なる方法で行われることを特徴とする請求項１乃至２記載のメモリシステム。

【請求項４】　前記個別情報は、前記記憶媒体内に記憶されるデータと異なるデータ記憶方式で記憶されることを特徴とする請求項３記載のメモリシステム。

【請求項５】　前記メモリシステムは、前記個別情報にアクセスするための情報を有し、前記情報を用いて、前記記憶媒体内に記憶されるデータと同一のデータ記憶方式で記憶される前記個別情報を、読み出すことを特徴とする請求項３記載のメモリシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は半導体メモリを用いたメモリシステムにおいて、その著作権保護の目的に利用されるものである。

【０００２】

【従来の技術】近年図１に示すようなフラッシュメモリカードがデジタルスチールカメラやＰＤＡ等の携帯情報機器の記憶媒体として注目されている。このメモリカードは薄型のプラスチックパッケージにわずかな窪みが設けられておりその窪みに２２ピンの平面電極を有するフラッシュメモリが埋め込まれている。本フラッシュメモリカードは専用のコネクタを介してホストシステムに電気的に接続され、データの入出力を行う。例えば、ＰＣカードアダプターを利用すると、フラッシュメモリカード上のファイルを簡単にＰＣへ転送することが可能である。

【０００３】

【発明が解決しようとする課題】しかしながら、上記フラッシュメモリ用いたメモリシステムにおいて、音楽データ等、著作権が存在するファイルも自由にコピーすることが可能で、著作権が侵害されるという問題点があった。本発明は上記問題点に鑑みなされたもので、フラッシュメモリカード等の利用に際し、著作権の保護が確保されるメモリシステムを提供することを目的とする。

2

【０００４】

【課題を解決するための手段】上記課題を解決するために、本願発明の請求項１に係る発明においては、着脱可能な記憶媒体と前記記憶媒体中に格納されたデータを使用するメモリシステムにおいて、前記記憶媒体には前記記憶媒体を個別に識別するための個別情報が保持され、前記記憶媒体中に格納されるデータを使用する際は、前記記憶媒体の個別情報を必要とすることを特徴とするメモリシステムを提供する。

【０００５】また、本願発明の請求項２に係る発明においては、着脱可能な記憶媒体と前記記憶媒体中に格納されたデータを使用するシステムにおいて、前記記憶媒体には、前記記憶媒体を個別に識別するための個別情報が保持され、前記記憶媒体中に格納されるデータには上記個別情報に関連付けられた情報が格納され、前記記憶媒体中に格納されるデータを使用する際は、前記記憶媒体の個別情報と前記データ中の関連付けられた情報の合致を確認後、前記システム中での前記データの使用を許可することを特徴とするメモリシステムを提供する。

【０００６】さらに、本願発明の請求項３に係る発明では、請求項１乃至２に係る発明において、前記個別情報の読み出しは、記憶媒体内のデータの読み出しと異なる方法で行われることを特徴とするメモリシステムを提供する。

【０００７】さらに、本願発明の請求項４に係る発明では、請求項３に係る発明において、前記個別情報が前記記憶媒体内に記憶されるデータと異なるデータ記憶方式で記憶されることを特徴とするメモリシステムを提供する。

【０００８】さらに、本願発明の請求項５に係る発明では、請求項３に係る発明において、前記メモリシステムが、前記個別情報にアクセスするための情報を有し、この情報を用いて前記記憶媒体内に記憶されるデータと同一のデータ記憶方式で記憶される前記個別情報を、読み出すことを特徴とするメモリシステムを提供する。

【０００９】

【発明の実施の形態】図１に示す小型のフラッシュメモリカードを例に取る。このメモリカードは薄型のプラスチックパッケージにわずかな窪みが設けられておりその窪みに２２ピンの平面電極を有するフラッシュメモリが埋め込まれている。本実施例では上記メモリカードに搭載されているフラッシュメモリとしてＮＡＮＤ型ＥＥＰＲＯＭと呼ばれるフラッシュメモリを例に説明する。このフラッシュメモリは市場でのデータの互換性を取るため、データの格納方法を規定した物理フォーマット仕様を規定する。

【００１０】１６ＭビットのＮＡＮＤ型フラッシュメモリの場合、図２に示すようにフラッシュメモリは５１２個の物理的なメモリブロックに分割されている。このブロックは消去時の最小単位となっている。１ブロックはさらにＰａｇｅ０～Ｐａｇｅ１５の１６ページに分割される。１ページは書き込みおよび読み出しの基本的な単位となる。１ページは２６４バイトから構成され、うち２５６バイトはユーザーデータ領域（データ部）、残りの８バイト（冗長部）はエラー訂正符号および管理情報等の格納に使用される。

【００１１】通常パソコン等ではデータはセクタ（５１２バイト）単位で管理されるため、本メモリカードでも５１２バイト単位でデータ管理を基本とし２ページをペアとする。データ領域の内部データ構成を図３に示す。未使用の正常ブロックは、データ部、冗長部とも“ＦＦｈ”に設定されている。下記に各々のバイトの意味を説明する。Ｄａｔａ　Ａｒｅａ－１は５１２バイトデータのうち、前半の０～２５５ｂｙｔｅのデータが格納される。Ｄａｔａ　Ａｒｅａ－２は５１２バイトデータのうち、後半の２５６～５１１ｂｙｔｅのデータが格納される。

【００１２】Ｄａｔａ　Ｓｔａｔｕｓ　Ａｒｅａはデータが正常でないことを示す。通常は“ＦＦｈ”だが、正常でないデータが書き込まれている場合に“００ｈ”が設定される。

【００１３】Ｂｌｏｃｋ　Ｓｔａｔｕｓ　Ａｒｅａはブロックの良・不良の状態を示す。通常は“ＦＦｈ”だが、不良ブロックの場合、“００ｈ”（初期不良ブロック）、“Ｆ０ｈ”（後発不良ブロック）が設定される。２ビット以上“０”があった場合は、不良ブロックであると判断する。なお、本データは同一ブロック内では全て同じ値を書き込む。

【００１４】Ｂｌｏｃｋ　Ａｄｄｒｅｓｓ　Ａｒｅａ－１はブロックの論理アドレス情報を示す。なお、本データは同一ブロック内では全て同じ値を書き込む。ＢｌｏｃｋＡｄｄｒｅｓｓ　Ａｒｅａ－２はＢｌｏｃｋ　Ａｄｄｒｅｓｓ　Ａｒｅａ－１のデータと同じ内容が書かれている。本メモリカードの制御では、データ更新時は消去済み領域に更新データを書き込み、元のデータが存在する領域を消去するという、追加書き込み方式を採用しているため、ある論理ブロックに対応するデータが存在する物理ブロックは、固定では無く、常にメモリ内を移動している。

【００１５】従って上述のごとく、物理ブロックの冗長部には自分がどの論理ブロックに対応するデータを保持しているかを示す論理ブロックアドレス情報を記憶している。通常は電源投入時に、全物理ブロックの該論理ブロックアドレス情報格納領域をサーチし、システムＲＡＭ上に、図４に示すような論理ブロックと物理ブロックの変換テーブルを作る。一度テーブルを作成した後は、該テーブルを参照すれば、論理ブロックに対応する物理ブロックがすぐに判断可能なため、全ブロックのサーチ動作は電源投入時１回で良い。当然のことながら、データの更新を行い、対応する物理ブロックの位置が変化した場合は、テーブルの更新作業を行い、次のアクセスに備える。

【００１６】ＥＣＣ　Ａｒｅａ－１は偶数ページデータ（２５６バイト）の３バイトＥＣＣコードである。ＥＣＣ　Ａｒｅａ－２は、奇数ページデータ（２５６バイト）の３バイトＥＣＣコードである。ここでＥＣＣ（Error Correction Code）とはエラー訂正のための符号をさす。システムはこのエラー訂正用の符号を利用し、読み出したデータにエラーがあるか否かを判定し、エラーが存在する場合、エラーを訂正することができる。

【００１７】図２を別の観点から書き下したものが図５になる。ここではＣＩＳ（Card Information Structure）というものを定義する。上述したように上記メモリカードでは市場での互換性を取るためにデータの格納方法を規定している。上記のＣＩＳはメモリカードが規定したデータ格納方法に準拠しているかどうかを判断するための識別領域である。ＣＩＳは有効なブロックのうち先頭のブロックに配置される。図５に示すように先頭のブロックが不良ブロックでなければ、ＣＩＳブロックはチップの先頭に配置される。もしチップの先頭のブロックが不良ブロックであれば、図６に示すように２番目のブロックに配置される。

【００１８】ＣＩＳは、図７に示す様に２個の領域に分割される。一つは固定のデータ領域（領域Ａ）である。この固定領域の先頭１０バイトを用いて、規定されたデータ格納方法に準拠しているか否かを判断する。システムは電源投入時、ＣＩＳブロックの先頭１０バイトを読み、その値が規定されたものと一致すれば、そのカード規定されたデータ格納方法に準拠しているものとし、処理を進める。もし規定された１０バイトが読み出せなければ、未知のフォーマット品という判断をし、データの破壊防ぐため以降の処理を中止する。

【００１９】ＣＩＳ領域は、システム（例えばアダプターカード中のコントローラ）のみが参照可能な領域で、一般のエンドユーザーが参照することはできない。例えば、アダプターカードを介してファイルを格納する場合、ファイルはファイルの管理領域（マスターブートセクタ、パーティションブートセクタ、ＦＡＴ、ディレクトリ等）およびファイルデータ本体を含めてＣＩＳ領域以外の場所を利用して格納される。従ってＣＩＳ領域はＰＣ上からは、特殊な手段を使用しない限り見えない。ＣＩＳのもう一つの領域（領域Ｂ）は任意のデータが設定可能な領域である。勿論エンドユーザーが任意のデータを設定できるわけではない。本フラッシュメモリカードが出荷される段階、もしくは特殊なツールによってデータが設定される。

【００２０】以下に上記のような規定のフラッシュメモリカード上においての著作権保護のための方法を１から１１の実施例を用いて具体的に説明する。著作権保護されるべきものとしては、例えばクラシック音楽やポピュラーミュージックといった音楽のデータ、英会話等の語学教材のデータ、文学や雑誌、新聞等の文字データ、公演やインタビュー、落語、漫才等の音声データ、アニメの人気キャラクター等のキャラクターデータ、風景等の画像データ、地図データ、音声ガイダンスデータ、地域情報データ、人物画等の画像データ等、法的に著作権が発生するものはすべて含まれる。また著作権が発生しないデータに対してなんらかのコピープロテクト等のデータ保護の需要がある場合も全く同様に取り扱うことが可能である。以下の説明においてはこれらを総称して著作物またはコンテンツ等と記載する。

【００２１】（第１の実施例）以下に、本願発明のメモリシステムの第１の実施例を説明する。本実施例は、フラッシュメモリにあらかじめ著作物を記憶した状態での販売を目的としたものである。

【００２２】著作保護のレベルは種々考えられるが、フラッシュメモリカードのＣＩＳ領域（図７の領域Ｂ、任意のデータ設定可能な領域）に識別コードをあらかじめ書き込んでおく。

【００２３】例えば、図８に示すように、第１の実施例のシステム機器（例えば、音楽再生機、画像表示機等）はフラッシュメモリーカードのＣＩＳの識別情報として“ＡＢＣ”の文字列を期待している。フラッシュメモリーカードとしてＣＩＳの識別情報に“ＡＢＣ”と書き込まれたもの（Ａ）と“ＤＥＦ”と書き込まれたもの（Ｂ）の２種類を想定する。実際の場合は、識別情報は３文字には限られず、文字数（英数字等もふくむ）は多い方が良い。ここでは説明を簡略化するため３文字の場合を例に説明する。図８のケースでは、システム機器はＣＩＳの識別情報として“ＡＢＣ”の文字列を期待しているので、（Ａ）のカードがシステムに挿入された場合は正常に使用が可能である。しかし（Ｂ）のカードは期待された識別コードを持っていないので本システム機器で使用できない。識別コードは一般には公開されないもので、この場合“ＡＢＣ”の識別コードを書き込んで販売されたメモリカードのみがシステム機器で使用可能となり、メモリカード内部の著作物の権利が保護される。

【００２４】（Ｂ）の場合、使用不可のレベルは多くのケースが想定できる。例えば音楽であれば、全く音楽が聞けないという状態のほかに、一部分だけ音楽が聞けるということが想定される。これは例えば、プロモーション用に一部分だけは聞けても良いといったケースに該当する。またシステムが画像表示機であれば、画像が全く見えないというプロテクト方法のほかに、一部分だけ画像が見える、スクランブルがかかったような（モザイク画面等）状態の画像のみが見える、小さいサムネイル画像等のみが見える、または正規のカードではあれば非常に高精細な画像が見え、それ以外の場合は精細度の低い粗い画像のみが見えるようにしても良い。また正規のカードであれば、ある機能が使え、それ以外であれば、ある種の機能が使用できないようにしてもかまわない。例えば音楽の場合、正規のカードでは、ＣＤプレイヤーと同様に頭出しの機能が使えるが、それ以外のカードではその機能が使用できない等、システム機器の機能になんらかの制限が加わっても良い。期待された正規の識別コードを有するカードとそれ以外のカードで、何らかの差があれば目的が達成されることになる。

【００２５】ただし、上記方法では、期待される識別コード“ＡＢＣ”が書き込まれたカードであれば、全て正規のカードとみなされ、記憶されているファイル自身の正当性が判断できない可能性がある。すなわち状況によっては“ＡＢＣ”の識別コードがあるカードを一度入手してしまえば、そのカード上にインタネット上の不正なＷＥＢサイトから入手した不正データが使用可能となるケースが想定される。また、システム機器製造時に期待する識別子を一義的に（本実施例の場合は、“ＡＢＣ”）決めてしまうと、“ＡＢＣ”以外の識別子を持って正規のカードを販売しようとしてもできない。このため、何らかの手段を用いて期待値の変更または追加をする機能を持つことが考えられる。例えば、正規のカード自身にシステム機器の期待値を変更、または追加するソフト等を入れておいて、それを用いてシステム機器の期待値を変更、追加する等の手段を持っても良い。またはシステム機器の期待値を変更、追加するソフトはシステム自身があらかじめ持っておき、変更値のみが何らかの約束事を持ってメモリカード上に存在させてもよい。もちろんカード上の情報によって期待値の変更をおこなうのではなく、例えばシステム機器がＰＣ等とケーブル等で接続されそれによって期待値が変更されるようなシステムでも良い。システム機器の出荷後、何らかの手法によって期待値が変更、追加される機能を持っていれば良い。

【００２６】（第２の実施例）次に、本願発明のメモリシステムの第２の実施例を説明する。本実施例も第１の実施例同様、フラッシュメモリにあらかじめ著作物を記憶した状態での販売を目的としたものである。

【００２７】第２の実施例の概要を図９に示す。本実施例ではフラッシュメモリカードのＣＩＳ領域に識別コードを記憶させると同時に、格納されるファイル自身にもＣＩＳに記憶させた識別コードと関連した情報を取り込む様にする。

【００２８】例えば、図９の（Ａ）に示すように、本メモリカードのＣＩＳの識別コードが“ＡＢＣ”の場合、カード中のファイルの中に識別コード“ＡＢＣ”に関連した情報を取り込む。　簡略化のために文字列“ＡＢＣ”をそのまま取り込むケースを想定する。

【００２９】システム機器はまずフラッシュメモリカードのＣＩＳ中の識別コードを読む。図９（Ａ）の場合“ＡＢＣ”が読み出される。次にシステムはメモリカード中のファイル中の所定の場所を読み出す。この時“ＡＢＣ”が読み出されれば、そのファイルを正規のファイルと認識する。

【００３０】仮に図９（Ｂ）のように、ファイルの所定領域から文字列“ＡＢＣ”ではなく例えば“ＤＥＦ”が読み出された場合は、そのファイルは、ＰＣ等を経由して別のフラッシュメモリカードからコピーされてきたファイルと判断し、システム機器上での使用を禁止または制限する。制限の具体的な内容については実施例の１で説明した内容に準ずる。

【００３１】実施例１と異なる点は、図９（Ｃ）に示すように、ＣＩＳ中の識別コードとファイル中の識別コードが一致すれば、システム機器の製造時のそれらの情報を知らなくても使用可能となる点である。例えば、システム機器が音楽の再生機の場合、ＣＩＳ領域中の識別コードは歌手名にまたはアルバム名等に相当する。本実施例は、システム機器は、新たな歌手が登場したり、あらたなアルバムが作られた後も、正規のフラッシュメモリカードに記憶される音楽であれば再生することができるので、問題なく販売することができる。

【００３２】本実施例は上記方法に限られない。フラッシュメモリーカードと著作物に適当な関係付けができれば良い。上記例では、ＣＩＳ領域中の文字列をそのままファイル中に取り込む場合を説明したが、発明の主旨に添った範囲で種々変更可能である。例えば、ファイル中に取り込む文字列はＣＩＳ領域に格納された文字列と必ずしも完全に一致する必要はない。“ＡＢＣ”に対して、逆転した“ＣＢＡ”と格納するようにしてもよいし、“ＡＢＣ”に対してアルファベット順に一文字ずらした“ＢＣＤ”としてもよいし、数文字ずらしてもよい。また、“ＡＢＣ”の文字に対しアルファベット順に数字を割り振り“１２３”としても良い。なんらかの規定に従い、ＣＩＳ領域中の識別コードと、ファイル中の識別コードとの関係が成立すれば本発明の主旨に合致していることになる。また、ＣＩＳ中の識別コードと文字数が一致している必要もない。“ＡＢＣ”に対し、“ＡＢＣＤＥＦ”または“ＡＢＣＡＢＣ”等文字数を変えて格納しても、何らかの規定が存在すれば全く問題ない。

【００３３】さらに信頼性を向上させる方法としては、単純にＣＩＳ領域中の識別コードをファイル中に格納するのではなく、ＣＩＳ領域中の識別コードに関連した情報を、ファイル中の他のデータと包括して暗号化するようなことをしても良い。単純にファイル中に格納した場合、別の識別コードを持つ数枚のメモリカードのファイルデータを比較することにより、識別コードに関連する情報の格納位置を特定される可能性がある。これを避けるために、ある程度の広い領域にわたって、暗号化する等の方法により、数枚のカードのファイルデータの相違個所を増やし、信頼性を向上できる。暗号化されたものを解く暗号キーは、システム機器側のＡＳＩＣ中等に持てば良い。または暗号キーそのものが、著作物と一緒に販売されるような形式でもかまわない。また、ＣＩＳ領域の識別子に関連付けられた情報は、各々にファイルに必ずしも入っている必要はない。著作物の内容に関連したした別のファイル（例えば、楽曲名が格納されたファイル）が統合的に持ってもかまわない。

【００３４】本実施例によって、例えば、正規の方法によって１枚の著作物の入ったメモリカードを購入した人物が、その著作物のファイルを一旦ＰＣ上に転送し、別の空のメモリカードにファイルを転送したとすると、ファイルの転送は正常にできるが、新たにファイルが転送された従来の空のメモリカード上では、ＣＩＳ領域の識別コードと転送されてきたファイル中の識別コードに関連付けられた情報との間に正当な関係が成り立たないのでシステム機器側で容易にそれが判断できる。これによって不正なコピーの使用が制限される。これは汎用のアダプターカード等を用いてＰＣへデータを転送する際、アダプターカード中のコントローラは標準のフォーマットに準拠しているか否かを確認するためＣＩＳ領域にアクセスするが、ＰＣ上のソフト等はＣＩＳ領域にアクセスすることは、特殊な方法を用いない限りできず、ファイルは転送可能でもＣＩＳ領域中の識別コード自身は他のメモリカードに転送されることが無いという仕組みを巧みに利用したものである。この例の概要を図１０に例を示す。正規のフラッシュメモリーカードにはＣＩＳ領域の識別コードとして“ＡＢＣ”が入っており、またファイル中の識別コードも“ＡＢＣ”である。このフラッシュメモリーカードのファイルを一旦ＰＣへ転送する。次にＰＣから別のフラッシュメモリーカードへファイルを転送する。この場合、転送先のメモリカードのＣＩＳ領域の識別コードは“ＤＥＦ“であり、転送されたファイル中の識別子”ＡＢＣ“とは一致しない、従ってシステム側は両者の不一致を認識し、不正にコピーされたものと判断する事が可能である。

【００３５】またＣＩＳ領域の識別コードは、著作物ごとに割り振られたコードでもかまわないし、フラッシュメモリカード１枚毎に固有、またはあるグループに対して固有のコードでもかまわない。単純に１バイトを識別コード領域に割り振った場合、００ｈからＦＦｈまでの２５６通りの設定が可能である。フラッシュメモリカード１枚ずつに順番に識別コードを書き込んでいった場合、２５６枚に１枚の確率で同じ識別コードを持つメモリカードが存在する事になるが、一般のエンドユーザーが、同じ識別コードを持った別のメモリカードを探し当てる確率は非常に小さい。識別コードをバイト数を増やすとその確率は限りなくゼロに近づける事ができる。１バイトのみ割振る場合でも、例えばアルバム毎にその番

号を割り振れば良い。仮に同じ識別コードを持ったメモリカードが発見されたとしても、互いにコピー可能なファイルは同一のファイルであり、両者とも正当に権利を買った著作物であるので、コピーをする事に全く意味がない。

【００３６】また、ファイル中の識別コードに関連付けられた情報とは広義である。ファイルが全体的あるいは部分的に暗号化されており、その暗号を解くカギが識別コードそのもの、または識別コードと関係付けられたものでも良い。この場合、識別コードとファイル中の識別コードに関連づけられた情報との、合致および不一致は、正常に暗号が解ける、解けないと言い換えることが可能である。

【００３７】以上のように、フラッシュメモリカードそのものと著作物の関連付けを行う事により、不正な著作物のコピーが防止される。

（第３の実施例）次に、本願発明のメモリシステムの第３の実施例を説明する。本実施例は、上記第１、第２の実施例では、フラッシュメモリカードにあらかじめ著作物を格納した状態で完売するケースを考えたが、本実施例は著作物の情報そのものの販売を目的とし、著作物を通常に販売されているフラッシュメモリカードにダウンロードするという形で入手するようなケースについてである。

【００３８】例えば、コンビニエンスストアや駅その他に専用の端末を置き、その端末を介して情報をダウンロードする。これらは専用の端末であり、ＣＩＳ領域を自由に参照、または書き替えをする事が可能である。すなわち上記専用端末上でデータを書き込んだ結果が、実施例の１および２で説明したあらかじめ著作物を格納したメモリカードの販売時の状態と同じになっていれば良い。すなわち情報の格納時にＣＩＳ領域の識別コードを書き替え、それと関連付けられた情報を取り込んだファイルとして著作物が格納されれば良い。

【００３９】この時、ＣＩＳ領域を書き替える事により従来格納していた著作物の利用は不可能となる。ただし、ＣＩＳ中の識別コードを複数個持つ様にすれば、複数回のデータダウンロードに対して既に存在していた正規のファイルの使用を中止することなく利用できる。

【００４０】データを書き込む専用端末としては、上記例に限られない。世の中に広く普及しているジュース等の自動販売機などにこの上記専用端末の機能を持たせてこれを利用しても良い。この場合、著作物の更新は自動販売機の販売物の補充の際、同時に行ってもかまわないし、ＰＨＳ機能等の無線機能または有線によって販売する著作物の更新をしてもかまわない。

【００４１】また、公衆電話等を用いることも可能である。公衆電話等にフラッシュメモリカードの挿入可能なコネクタをつけ、公衆回線を利用し著作物の配布を行っても良い。ＰＨＳや携帯電話等を介しても同様の事が想定可能である。または衛星放送等やＣＡＴＶからデータを受信するようなケースも想定可能である。勿論ＰＣでも同様の事は可能である。ＣＩＳ領域のデータを外部に読み出すことにできる機能を持ったツールを用意してもよい。ＰＣのＵＳＢポート、シリアルポート、またはプリンタポート、ＩＳＡバススロット等に接続可能なツールを専用のソフトウェアで制御すれば、専用端末と同様にＣＩＳ領域にアクセスし識別コード等を参照したり、変更したりすることも可能である。アダプターでも上記説明はＰＣカードＡＴＡインタフェースのようにＰＣに標準でデバイスドライバを持った汎用のアダプターを想定したが、例えばＰＣカードＡＴＡインタフェースには準拠せずユーザーが自らデバイスドライバをインストールするようなタイプのアダプターカードで、ＣＩＳ領域にアクセス可能な物をまたは、同様の機能をもつものを使用し、専用のダウンロードソフトを利用すれば良い。

【００４２】また本発明は図１に示したフラッシュメモリーカード以外にも適用が可能である。例えば、PCカードＡＴＡインタフェースに準拠したフラッシュメモリカードの場合を次に説明する。

【００４３】ＰＣカードＡＴＡインタフェースはＩＤＥ仕様のハードディスクのプロトコルをそのままＰＣカードに適用したものである。一般的に上記ＡＴＡカードの内部にはフラッシュメモリのほかに、コントローラやバッファ用のＲＡＭ、ファームウエアを格納するための小規模のフラッシュメモリ（コントローラ内蔵されていても良い）等が搭載されている。

【００４４】上記実施例のＣＩＳ領域の識別コードに相当するものをこのＡＴＡカード中に格納する方法は多種考えられる。例えば、ＰＣカードにはアトリビュートメモリ空間が定義されており、ホストシステムはこの領域を参照することにより、カードの種別（例えば、ＡＴＡカード、モデムカード、ＬＡＮカード等）を判断している。このアトリビュートメモリ空間の内容はタプルと呼ばれ、ＰＣカードスタンダード等で標準化されている。この仕様中には、カードベンダーが、ベンダー情報や製品情報を設定できる領域がある。この領域を使用すれば、上記実施例の主旨に添った動作は可能となる。この場合の設定値は、コントローラ中の不揮発性メモリ上に持っても良いし、コントローラと接続されたフラッシュメモリ等の不揮発性メモリに持っても良いし、カード中のファイル格納用のメインのフラッシュメモリ中に持ってもよい。また上記アトリビュートメモリ空間以外でも同様の動作が可能である。ＡＴＡのプロトコルの中には、Identify Driveというコマンドがある（Hex Code Ech）。本コマンドはハードディスクとしての仕様値（例えば、セクタ数、シリンダ数、ヘッド数）をホスト側に通知するためのコマンドである。本コマンドの返り値の中にはモデルナンバーや、内蔵マイクロコードのバージョン等を格納する領域がある。本領域に上記実施例のＣ

ＩＳ領域の識別コードに相当するものを格納すれば良い。上述のごとくその値をＡＴＡカード中の何所に格納するかは任意である。またその値は汎用性を考え書き換えが可能な状態でも良いし、セキュリティを高める目的で消去や書き替えが不可能な状態としてもよい。

【００４５】また、新たなベンダーユニークなコマンドを使用してもかまわない。ＡＴＡのプロトコルで規定されている以外のコマンドを用いて、上記実施例のＣＩＳ領域の識別コードに相当する値を出力する使用にしてもよい。例えば、Ｆ３ｈを識別コード読み出しコマンドと設定しても良いし、Ｆ３ｈ－Ｆ４ｈ等の複数回のコマンド入力を必要としても良い。カードからの出力方法としては、１バイト目から識別コードを出力しても良いし、１バイト目もしくは規定されたバイト数で本コマンドをサポートしている事を示す何らかの値（例えばＡａｈ）等を出力するようにしても良い。勿論本コマンドをサポートしているか否かを判断するための別コマンドを用意してもかまわない。識別子のバイト数は任意である。他のコマンドとの整合性を持たせるため１セクタ（通常５１２バイト）分のデータを読み出す仕様でも全くかまわない。また従来から存在するコマンドを使用して意味合いを拡張するようにしてもかまわない。例えば、Read long コマンド(22h/23h)は、５１２バイトデータ転送の後、ドライブからホストにＥＣＣバイトを含みデータを転送する。このバイト中に識別コードに相当する情報が入っていても良い。また、ある特定のセクタにアクセスすると上記識別コードに相当するものが出力されるように規定をしても良いし、サポートしているアドレス空間（セクタ数）以外のセクターをアクセスすることによって同情報が得られるように決めても良い。また、カード中に搭載されているコントローラがみずから識別コードとファイル中に格納された上記識別コードに関する情報とを比較し、異なる場合はファイルの出力を禁止するようにしても良い。以上にようにメモリカードが何らかの方法によって識別コードを格納し、さらにファイル中にも同識別コードに関連付けられた情報が取り込まれ、両者が比較できるような機能をシステム全体として持つ事ができれば良い。

【００４６】また、本実施例の適用は上記ＡＴＡカードのみに限られない。コントローラを搭載していない各種のメモリカード、ＡＴＡ仕様とは異なるタイプのコントローラ（必ずしもＣＰＵを搭載している必要はなく、比較的な簡単なＡＳＩＣ等で構成されていても良い）を搭載したカード、さらにはフラッシュメモリ以外のメモリ（ＦＲＡＭ、ＳＲＡＭ、ＭＲＯＭ、ＤＲＡＭ等）を搭載したカードでも良いし、各種のメモリが混載されていても良い。フラッシュメモリも図１に示したメモリカードで使用されているＮＡＮＤ型フラッシュメモリの他、ＡＮＤ型、ＮＯＲ型、ＤＩＮＯＲ型、フラッシュメモリ種別にこだわらないし、バイト型ＥＥＰＲＯＭ、シリアルＥＥＰＲＯＭ、ＥＰＲＯＭ等フラッシュメモリ以外の不揮発性メモリに対しても適用可能である。またＣＤＲＯＭ、ＤＶＤ、ＭＤ、ＬＤ、ＨＤＤ、ＦＤといった半導体以外の記憶媒体に対しても全く同様に議論することが可能である。記憶媒体と記憶媒体に格納されたファイルがあり、記憶媒体中に固有の識別コードが記憶され、ファイル中に上記識別コードに関連付けられた情報が格納されていれば、本発明の主旨を満足している。

【００４７】また、ファイル中の識別コードに関連付けられた情報とは広義である。ファイルが全体的あるいは部分的に暗号化されており、その暗号を解くカギが識別コードそのもの、または識別コードと関係付けられたものでも良い。この場合、識別コードとファイル中の識別コードに関連づけられた情報との、合致および不一致は、正常に暗号が解ける、解けないと言い換えることが可能である。

【００４８】識別コードの保持方法、両者の情報の比較方法、および相違が有った場合の処理の方法については非常に広い任意性を有する。（第４の実施例）次に、本願発明のメモリシステムの第４の実施例を説明する。本実施例は、上記実施例１から３の場合の信頼性をさらに向上させる方法を以下に説明する。本実施例は、実施例１から３と組み合わせても使用可能であるし、また実施例４単独で使用することも可能である。本実施例は既に説明した標準的なデータの格納仕様（物理フォーマット）の仕組みを利用するものであり、標準的な物理フォーマットで正常に格納された状態と一部異なる状態を意図的に形成することを特徴とする。

【００４９】例えば、Ｄａｔａ　Ｓｔａｔｕｓ　Ａｒｅａを使用する方法がある。記述のようにＤａｔａ　Ｓｔａｔｕｓ　Ａｒｅａは格納されている情報が正常でないことを示す。通常は“ＦＦｈ”だが、正常でないデータが書き込まれている場合に“００ｈ”が設定される。例えばアダプターカードの場合Ｄａｔａ　ＳｔａｔｕｓＡｒｅａにマークが施されているセクタ（データが正常でない）にホストシステムからアクセスが有った場合はエラーを返す。従ってＰＣ等でＤａｔａ　Ｓｔａｔｕｓ　Ａｒｅａにマークがついた領域を含むファイルを転送することはできない。このことを使用して不正なコピーを防止することが可能である。

【００５０】図１１に本実施例の概要を示す。ファイルＡはファイル中のデータのいずれかにＤａｔａ　Ｓｔａｔｕｓ　Ａｒｅａにマークが施されているものである。ファイルＢのＤａｔａ　Ｓｔａｔｕｓ　Ａｒｅａは正常である。例えばあらかじめメモリカードに著作物を格納した状態で販売するケースを想定するとファイルＡがそれに該当する。著作物を格納する段階でＤａｔａ　Ｓｔａｔｕｓ　Ａｒｅａにマークを付与してファイルを格納する。この状態で汎用のアダプターカード等を利用してＰＣ上へファイルを転送しようとした場合、ファイルＡ

の格納領域にアクセスがあると、アダプターカード中のコントローラは該当データが正常でないと判断し、ホストに対してエラーを返す。この時例えばＰＣ上では「ドライブに異常がある」とのメッセージ等が画面上に表示され、ファイルの転送は中断される。Ｄａｔａ　Ｓｔａｔｕｓ　Ａｒｅａにマーキングの無いファイルＢは自由にＰＣへデータ転送が可能である。

【００５１】このように、意図的にデータが正常でない事を示すマークを付与した状態でファイル格納をする事により、著作物の不正なファイルコピーを防止することができる。勿論システム側（例えば音楽再生機）は、Ｄａｔａ　Ｓｔａｔｕｓ　Ａｒｅａのマークが意図的につけられたものであることを理解し、正しいデータが格納されているものとして取り扱う。従ってＤａｔａ　Ｓｔａｔｕｓ　Ａｒｅａに意図的にマークをつける場合はあらかじめどの領域にマークをつけるのか決めておく必要がある。マークの付与位置は様々なケースが想定できる。例えば、各ファイルにマーク施す場合を考える。勿論ファイル全体の各セクタに対しマークを施しても良い。また、一部分のみ施しても良い。例えばファイルの第何番目のセクタをその目的に使用すると決めておく方法である。マークを施すデータをあらかじめ設定しても良い。例えば、１セクタのデータをすべてＦＦｈとし、そのセクタに対しマークを施す仕様にしておいても良い。マークを施す位置はファイル中とは限られない。例えば、ＤＯＳのファイル管理領域でもよい。マスターブートセクタ領域やパーティションブートセクタ、ＦＡＴ領域、ルートディレクトリ領域、サブディレクトリ領域等にマークを施してもよい。マスターブートセクタ領域等にマークをつけるとＰＣ上からはドライブとして認識できなくなるため、ファイルの転送は不可能となる。Ｄａｔａ　Ｓｔａｔｕｓ　Ａｒｅａのマークは、リード動作に対して有効である。新たに同領域に書き込み命令が発行されれば、新しいデータが書き込まれ、Ｄａｔａ　Ｓｔａｔｕｓ　Ａｒｅａのマークは消滅する。従って、音楽再生用に本発明によってコピー防止機構がついたカードも、該当のファイルが不用になれば、別のファイルを書き込んでも良いし、別のシステムで再利用することも可能である。本実施例は、本来の正常な状態とは一部異なるなる状態を意図的に形成し汎用のシステムがその状態を判断することによって不正なコピーが防止できるという主旨の範囲で種々変更して適用可能である。別の言い方をするとデータ本体に付加的に記憶された管理情報の内容によりデータの読み出し動作を許可したり禁止したりする。ＡＴＡアダプターカードでは内蔵のコントローラが該当領域を見てエラーを返すが、コントローラを内蔵しないタイプのアダプターカード等ではＰＣ上のデバイスドライバーが同様の判断することは言うまでもない。エラーの返し方としても各種の方法が考えられる。ＡＴＡアダプターカードの場合は、訂正不可能な読み取りエラーが発生した旨ホストに通知しても良いし、不正なコマンドが入力された旨通知（コマンドアボート）しても良いし、指定されたセクタが発見できなかった等を意味するエラーコードを返しても良い。エラーの返し方としては任意である。

【００５２】次に、Ｂｌｏｃｋ　Ｓｔａｔｕｓ　Ａｒｅａを使用する方法を示す。記述のごとくＢｌｏｃｋ　Ｓｔａｔｕｓ　Ａｒｅａはブロックの良・不良の状態を示す。通常は“ＦＦｈ”だが、不良ブロックの場合、“００ｈ”（初期不良ブロック）、“Ｆ０ｈ”（後発不良ブロック）が設定される。２ビット以上“０”があった場合は、不良ブロックであると判断する。

【００５３】システムは通常は電源投入時に、全物理ブロックの該論理ブロックアドレス情報格納領域をサーチし、システムＲＡＭ上に、図４に示すような論理ブロックと物理ブロックの変換テーブルを作る。一度テーブルを作成した後は、該テーブルを参照すれば、論理ブロックに対応する物理ブロックがすぐに判断可能なため、全ブロックのサーチ動作は電源投入時１回で良い。当然のことながら、データの更新を行い、対応する物理ブロックの位置が変化した場合は、テーブルの更新作業を行い、次のアクセスに備える。図４に示されるのテーブル作成時の全ブロックサーチの際、システムはまずＢｌｏｃｋ　Ｓｔａｔｕｓ　Ａｒｅａを最初に参照する。ここで、Ｂｌｏｃｋ　Ｓｔａｔｕｓ　Ａｒｅａにマークが施されていると（電気的に不良なブロックで、消去できないもしくは書込みができない、または訂正不可能なエラーが発生した等の症状を持っている）、システムは該当ブロックに対してＢｌｏｃｋ　Ａｄｄｒｅｓｓ　Ａｒｅａ等を参照してテーブルを作成するルーチンを中止し次のブロックへ処理を移す。従って次の電源再投入まで不良ブロックが再びアクセスされることはない。ゆえに汎用のシステムではＢｌｏｃｋ　Ａｄｄｒｅｓｓ　Ａｒｅａにマークのついた不良ブロックの内部データを参照することはない。

【００５４】この仕組みを利用して著作物の保護を行う方法を以下に記す。すなわち不良ブロックの登録されたブロックに記憶された情報を著作権保護に利用する。例えば、上記実施例１から３にて記載したように、メモリカードの識別情報等を見かけ上の不良ブロックに格納する。図１２に概要を示す。システム（例えば音楽再生機）は、不良ブロック内に記憶された識別コードとファイル中に埋め込まれた上記識別コードと関連付けられた情報との合致を期待している。図１２（Ａ）のカードでは、不良ブロック内の識別コードは“ＡＢＣ”でファイルに埋め込まれた識別コードも“ＡＢＣ”であり両者が一致するので、本メモリカードに記憶されている著作物は正規の著作物と判断することが可能である。一方、図１２の（Ｂ）および（Ｃ）は不良ブロック内の識別コードとでファイルに埋め込まれた識別コードに差異が見ら

れるため、記憶されている著作物が不正に入手されたものと判断して処理に制限を加える。以上のように不良ブロック内の識別コードと、ファイル中に埋め込まれた識別情報に関係づけられた情報を比較検討することで、正規の著作物を判別する事ができる。

【００５５】メモリカードの中には先天性もしくは後天性の不良ブロックが存在している。識別コードが格納されている不良ブロックを特定するための方法は様々考えられる。例えば識別コードが入っていることを確認するためのデータが該当ブロックに記憶されていれば良い。例えば、ブロックの先頭ページの最初のバイトに“ＡＡｈ－５５ｈ”といったデータを書いておく。または識別コード自身を複数（１セクタもしくは複数セクタ）個書き込んでも良いし、識別コードをそれを用いてなんらかの計算を実行した（例えばパリティや、チェックサム）結果と共に格納しても良い。真の不良ブロックにたまたま存在しているデータが、偶然識別コードを格納する方法と一致するか確率が低くなる手法が盛り込まれてさえいれば良い。また、チップの先頭または最後に近いブロックから使用する等のルールを決めておくと該当ブロックが見つかるのが早い。見かけ上の不良ブロックに格納する情報としては、上記識別コードに限られない。例えばシステムが音楽再生機の場合、該当のメディアで聞く事のできるファイル名に関連付けられた情報が入っていて、それ以外の楽曲ファイルの再生は禁止するようにしてもよい。汎用のシステムがアクセスすることのない領域を意図的に形成し、その領域に格納したデータを基に著作物の正当性が確認可能な手段を持つ事が本発明の本質である。

【００５６】上述のごとく、Ｄａｔａ　Ｓｔａｔｕｓ　ＡｒｅａおよびＢｌｏｃｋ　Ｓｔａｔｕｓ　Ａｒｅａについて説明した、図３中に示す他の領域においても同様の動作が可能である。現在、将来の使用のためＲｅｓｅｒｖｅｄされている４バイトの領域も同様の主旨で使用する事は可能であるし、同様にＢｌｏｃｋ　Ｓｔａｔｕｓ　Ａｒｅａを使用することも可能である。Ｂｌｏｃｋ　Ｓｔａｔｕｓ　Ａｒｅａは各セクターに２個づつ同じ物が格納されており、例えば１６メガビット（２メガバイト）品では1 個のブロック内に１６個のエリアが存在する。通常システムが各ブロックの先頭または最後のセクタのＢｌｏｃｋ　Ａｄｄｒｅｓｓ　Ａｒｅａしか参照しない。従ってブロック内の中間セクタのＢｌｏｃｋ　Ａｄｄｒｅｓｓ　Ａｒｅａをこれまで説明を加えてきたものと同様の主旨によって使用することも可能である。上記Ｒｅｓｅｒｖｅｄ　ＡｒｅａやＢｌｏｃｋ　Ａｄｄｒｅｓｓ　Ａｒｅａの利用も、標準的な物理フォーマットで正常に格納された状態と一部異なる状態を意図的に形成することを特徴とする面ではＢｌｏｃｋ　Ｓｔａｔｕｓ　Ａｒｅａもしくは、Ｄａｔａ　Ｓｔａｔｕｓ　Ａｒｅａの使用方法と同じ主旨である。

【００５７】図３の各エリアのうち、ＥＣＣ符号のエリアのみはまだ説明を加えていないが、勿論この領域は上記例と同様に使用する事も可能であるが、また別の観点から使用する事が可能である。

【００５８】図１に示したフラッシュメモリカードではＥＣＣ（エラー訂正コード）が使用されている。ＥＣＣの方式の詳細については、ここでは本発明の主旨と直接関係ないので省略するが、１セクタに対し（正確には１セクタを２分割し、各々の２５６バイトに対し）２ビットエラーの検出および１ビットエラーの訂正の能力を持つＥＣＣを使用している。

【００５９】ここでは、これまでの議論と同様にフラッシュメモリカードに著作物をあらかじめ格納した状態での販売、または専用端末からのダウンロードする場合を想定する。例えば、意図的にＥＣＣエラーが発生した状態で著作物を格納する。この場合概要を図１３を用いて説明する。ここでは説明を簡略化するためファイル名の格納領域に意図的にＥＣＣエラーを発生させた状態を作り出す。ファイル名を“ＡＢＣ”とすると実際のデータとしては４１ｈ、４２ｈ、４３ｈと格納されている。ここで、ＥＣＣの符号を調整し、“ＡＢＣ”の領域にあたかもエラーが発生しているような状態とする。例えば、ＥＣＣ符号で訂正されると“ＡＣＣ”（４１ｈ、４３ｈ、４３ｈ）となるように調整する。システム（例えば音楽再生機）中のコントローラ等は、意図的にＥＣＣエラーが発生している個所を認識している。従って、システムは４１ｈ、４３ｈ、４３と書き込んであるファイルのみが正規の著作物と認識する。ここでアダプターカード等を介してファイルをPC上へ転送し、さらに別のメモリカードにファイルを転送するとする。この場合、正規のメモリカードからＰＣへファイルが転送される際、アダプターカード中のコントローラによって、意図的に形成されたエラーが自動的に訂正され、ファイル名称が“ＡＢＣ”から“ＡＣＣ”に変ってしまう。最終的に別のメモリカードに転送されたファイルの名称は“ＡＣＣ”となる。このメモリカードをシステムに挿入した場合、システム中のコントローラはファイル名称が期待している“ＡＢＣ”ではないので該当ファイルが不正にコピーされたものであるとの認識が可能である。ここでは説明を簡略化するためファイル名称を例にあげたが、ファイル名称はエンドユーザーがＰＣで容易に書き換えることができるので実際に本実施例を適用するのは、別の領域がふさわしい。意図的にエラーを仕込んでいる場所をあらかじめ規定しておけば問題ない。また意図的にエラーを発生される個所は１ヵ所に限られず複数個所でもかまわない。マークを施す位置はファイル中でも良い。例えば、ＤＯＳのファイル管理領域でもよい。マスターブートセクタ領域やパーティションブートセクタ、ＦＡＴ領域、ルートディレクトリ領域、サブディレクトリ領域等にマークを施してもよい。汎用アダプター等を介し

てＰＣへ転送されたファイルが、転送元の正規のファイルと何らかの差異を持ってコピーされれば、その主旨を満足している。

【００６０】上記実施例では訂正可能な１ビットエラーを意図的に発生させたが、訂正不可能な２ビット以上のエラーを意図的に発生させても良い。この場合、汎用のアダプターカード等を利用してファイルをＰＣへ転送しようとするとアダプターカード中のコントローラが、訂正不可能エラーを検知しＰＣへエラーの発生を通知しファイルの転送は中断される。結果として正規のメモリカードからファイルがコピーされるのが防止されたこととなる。勿論、上述のように２ビットエラーを意図的に発生させる場所は任意である。また３ビット以上のエラーを意図的に発生させた場合、エラーが検知されない、もしくは誤訂正される可能性がある、この仕組みを利用しても良い。また、ファイル中の識別コードに関連付けられた情報とは広義である。ファイルが全体的あるいは部分的に暗号化されており、その暗号を解くカギが識別コードそのもの、または識別コードと関係付けられたものでも良い。この場合、識別コードとファイル中の識別コードに関連づけられた情報との、合致および不一致は、正常に暗号が解ける、解けないと言い換えることが可能である。

【００６１】（第５の実施例）次に、本願発明のメモリシステムの第５の実施例を説明する。上記実施例１から４では、フラッシュメモリーカードに著作物をあらかじめ記憶させた状態での販売を考えてきたが、本実施例では、インタネット上からＰＣを介してファイルがダウンロードされる場合を想定し、特に既存のハードの使用が前提となる。例えば、汎用のアダプターカードを想定する。インタネット上からいったんＰＣのハードディスク上にファイルとしてダウンロードされ、該当ファイルを汎用アダプターを介してフラッシュメモリーカードに転送する場合、上記実施例１から４のような物理フォーマットの階層を利用した著作権保護の仕組みは使用できないケースが想定される。なぜなら、例えばＰＣからアダプタカードを介してファイルをフラッシュメモリカードに転送する際、ＰＣはメモリカードのＣＩＳ領域を参照することはできないからである。したがってＣＩＳ領域中の識別コードをファイル中に取り込むような操作は不可能となる。

【００６２】このようなダウンロードシステムでの著作権保護の概要の仕組みを図１４に示す。ここでシステム機器（例えば音楽再生機）にはシステム機器個々に固有の情報（以下説明を簡便化するため単に機器番号と記す）が付与されている。機器番号は１台１台を完全に識別可能なものが望ましいが、２台の機器があったときにその２台が同じ機器番号を持っている確率が小さければ良い。また連続的な番号でも良いし、乱数のようなものでも良いし、それらはメーカーの製造番号のようなものと一体化していても良い。機器番号の付与方法は種々考えられる。システム機器の外装部分に金属プレートを貼り付けるような方法でも良いし、内装部分（例えば電池格納部分）にあっても良い。またシステム機器のディスプレイ上に表示されるような仕組みでもかまわないし、音声で案内されても良いし、取り扱い説明書、保証書等に記載されても良い。すなわち、エンドユーザーがシステム機器の機器番号を認識できる仕組みがあれば良い。さらにこの機器番号はシステム機器内部のコントローラが自由に参照可能であることが必要である。例えば、bコントローラ内部の不揮発性メモリ上に記憶されていても良いし、バスを介してコントローラと接続される不揮発性メモリ上に格納されていても良い。電池でバックアップされるならば、ＳＲＡＭ、ＤＲＡＭ等のメモリ上に記憶されていても良い。またディップスイッチ等の機械的な手段によって記憶されていても良い。コントローラの相当するものが電気的な手段によって参照できれば良い。

【００６３】インタネット上からのダウンロード方法を具体的に記す。音楽配信を行うウェブ（ＷＥＢ）上で、ダウンロードしたい楽曲を選定し、所有しているシステム機器（音楽再生機）の機器番号を入力する。その後、ファイル中に機器番号もしくは機器番号と密接に関連した情報等が取り込まれた形でユーザーのＰＣのハードディスク等にダウンロードされる。もちろんクレジットカード番号の入力などの方法で適正な課金がされる。

【００６４】結果的にエンドユーザーの手元には、所有しているシステム機器の機器番号に関連する情報が取り込まれたファイルが例えばハードディスク上に残ることになる。ユーザーは例えば汎用のアダプターカードを用いてファイルをフラッシュメモリーカードに転送する。このフラッシュメモリーカードがシステム機器に挿入された場合システムは、ファイル中の機器番号に関連付けられた情報の格納領域を参照する。もしシステム自身の機器番号とファイル中の機器番号に関連した情報に合致が確認された場合、システムはそのファイルが正規のファイルであることを認識し楽曲の再生を許可する。合致が得られなければ不正に入手されたファイルと認識し楽曲の再生を禁止する。したがって本実施例に従えばインタネットを通じて入手したファイルは特定のシステム機器のみで使用することが可能である。上記のフラッシュメモリーカードは他のシステム機器に挿入した場合、機器番号とファイル中の情報が合致しないので使用することはできない。したがってこの実施例でのデータ配信は特定のフラッシュメモリーカードに対して実行されたのではなく、特定のシステム機器向けに実行されたことになる。ここでハードディスク上に残っているファイルを別のフラッシュメモリーカードに転送した場合を考える。この場合ハードディスク上にあるファイルは完全な状態で他のフラッシュメモリーカードに無限にコピーす

ることが可能である。ただし、それらのメモリカードの中に転送されたファイルの中には、そのファイルが動作するシステムとして元々のシステムの機器番号が取り込まれている。したがってコピーは無尽蔵にできるものの、それを使用できるシステムはあくまで特定のシステム機器に制限されており、著作権が保護されることになる。

【００６５】上記実施例では、あるファイルはある特定のシステムのみで使用することができたが、複数のシステムで使用できるようにしても良い。インタネットからダウンロードする際、上記実施例では１個のみの機器番号が入力可能であったが、少なくても２個以上の機器番号を設定可能にしても良い。１個人が複数の機器を有している場合を考えると有効である。使用可能な機器番号の他、使用を禁じる機器番号も格納できるような手段、例えば管理フラグを持っても良い。例えば当初２台の機器が登録されていた場合に、そのうち１台システム機器上でのファイルの使用権を放棄するような場合に、機器登録を抹消するような動作が可能となる。使用可能な機器の登録数を増やす場合の手段としては、登録数を増やしたファイル自身がインタネット上から転送されて来ても良いし、ハードディスク上等に保管されているファイルに対し、登録機器の追加の操作を行うソフトウエアのみが転送されてきても良い。すなわちシステム機器の機器固有の番号と、該当機器番号に関連つけられた情報を盛り込んだ形で入手されるファイルが存在し、システム機器が両情報の合致を確認して動作の可否を判定するシステムにおいて、なんらかの手段により、機器番号の追加、抹消等、登録機器数の変更が可能な手段を持てば本発明の主旨に合致する。

【００６６】上記実施例では、ファイルを使用する機器の数に変動があった場合に、ファイルの中に格納されたサポート機器情報を更新することによって対応したが、システム機器側で、その機器番号を変更するような方法を取っても良い。機器番号１００番の機器と２００番のシステム機器をエンドユーザーが所有していた場合、機器番号１００番を前提に何らかの方法（例えばインタネット上から）で入手したファイルを数多く使用していたとする。エンドユーザーがこれらのファイルを２００番の機器で使用したいと考えた場合、上記実施例で説明したファイル中のサポート機器番号の更新によって対応するのは、ファイルの数量によっては大変な手数が必要となる可能性がある。この場合２００番の機器番号を１００番に変更可能な手段を持てば良い。すなわち２台の機器番号が統一されれば、ファイルの種類は１種類で共通化して使用することが可能である。機器番号変更の具体的な手段としては各種の方法が考えられる。例えば、システム機器の入力キーの操作によって実現されても良いし、機器番号変更のソフトウエアがインタネット上から配信され、それをフラッシュメモリーカード上に転送し、システム機器上で該当ソフトを実行させることにより機器番号が変更されても良い。無制限に機器番号が変更可能なことは問題があるので、上記の機器番号変更ソフトウェアは、変更されるシステム機器の元々の機器番号および変更する機器番号を特定した形で配信されれば良い。また単純な変更だけではなく、１台のシステム機器が複数の機器番号を持つような形にしても良い。例えば、１００番の機器番号を持つ機器が、２００番の機器番号をあわせ持つような形にすれば、１００番用のファイルの他、元々２００番の機器で使用していたファイルもあわせて使えるようになる。

【００６７】このように、本実施例の主旨は、システム機器に固有の機器番号情報等が、変更、追加、削除等を含めて更新できることを特徴としている。また機器番号が一個に固定されず、複数の機器番号を持つような形にすることも特徴である。また機器番号の変更は、システム機器の製造または販売サイドで行うようにしても良い。例えば所有しているシステム機器が故障し新たにシステム機器を購入する場合、上記製造または販売サイドに元のシステム機器を送付した上で、同じ機器番号を持った新しいシステム機器を購入できるようなサービスを設けても良い。追加でシステム機器を購入する場合も、現在システム機器を所有していることを証明する手段と共に、新しく購入するシステム機器に対しこれまで所有している機システム器と同じ機器番号が設定されたものを購入できるようにしても良い。

【００６８】また、ファイル中の識別コードに関連付けられた情報とは広義である。ファイルが全体的あるいは部分的に暗号化されており、その暗号を解くカギが識別コードそのもの、または識別コードと関係付けられたものでも良い。この場合、識別コードとファイル中の識別コードに関連づけられた情報との、合致および不一致は、正常に暗号が解ける、解けないと言い換えることが可能である。

【００６９】（第６の実施例）次に、本願発明のメモリシステムの第６の実施例を説明する。上記１から５の実施例は、フラッシュメモリーカードやシステム機器を個別に認識する手法を取ったが、本実施例では、ユーザー個人を認識させるというものである。

【００７０】説明を簡略化するため、ここでは個人の生年月日を例に説明する。個人の識別情報としては、生年月日のみに限られない。氏名でもかまわないし、任意に設定される暗証番号でも良いし、クレジットカードの会員番号、社会保障番号等でもよく、また１００％の確率で他人と異なっている必要も無い。ある確率で他人と異なっていれば、良い。システム機器（ここでは音楽再生機を例に取る）を購入したエンドユーザーがインタネット上から音楽ファイルを購入する場合を例に取る。

【００７１】システム機器には、上記の個人識別情報が取り込まれている。取り込む方法は任意である。店でシ

ステム機器を購入する際、販売者側が設定しても良いし、購入後エンドユーザーが自ら設定してもかまわない。エンドユーザーはインタネット上からファイルを購入する際、指定された個人識別情報を設定する。（例えば生年月日）ファイルの中には生年月日もしくはそれに関連付けられた情報が取り込まれるようにする。システム機器は、機器上に保持されている個人識別情報とファイル中に取り込まれた個人識別情報を比較し、合致がみられる場合にのみ音楽の再生を許可する。本実施例の特徴は、ファイルに個人の識別情報が取り込まれる事により、例えばエンドユーザーが複数のシステム機器を有していた場合、１つのファイルを全ての機器上で共通に使用する事が可能となる。エンドユーザーがシステム機器を追加購入する場合や、複数所持している機器いずれかに故障が発生した場合を想定すると非常に利便性が高い。生年月日の代わりに個人の氏名を使用した場合も同様である。ファイルはハードディスクから複数のフラッシュメモリーカードに自由にコピーすることが可能である。ただし再生は、ファイルを購入した個人が所有するシステム機器以外では再生することができない。同じ生年月日を持つ人や、同姓同名の人の間では再利用可能であるが、その確率が非常に低い。勿論、複数の個人識別情報を組み合わせて使用すれば（生年月日と氏名）、その確率が事実上ゼロとなり、著作権が保護される。また機器上の個人識別情報や、ファイル中の個人識別情報は、追加、変更、削除などができるようにしておく。婚姻等により氏名が変更になった場合や、権利を他人に譲渡することが可能となる。

【００７２】また、ファイル中の識別コードに関連付けられた情報とは広義である。ファイルが全体的あるいは部分的に暗号化されており、その暗号を解くカギが識別コードそのもの、または識別コードと関係付けられたものでも良い。この場合、識別コードとファイル中の識別コードに関連づけられた情報との、合致および不一致は、正常に暗号が解ける、解けないと言い換えることが可能である。

【００７３】（第７の実施例）次に、さらにセキュリティーを高める方法として、本願発明のメモリシステムの第７の実施例を説明する。これまでの実施例は、一般のエンドユーザーを対象に著作権保護の方法を記載したものだが、本実施例では、悪意を持った第三者が不正行為を実行するのを防止する観点に立っている。例えば、フラッシュメモリカードの電気的なインタフェース仕様はインタネット上の情報等を介して一般に公開されている。従ってメモリカード中のデータをファイル単位ではなく、単なるバイナリーデータの集合体として、あるメモリカードから、別のメモリカードへバイト単位で忠実にデッドコピーするような特殊ツールを作成することが技術的には不可能ではない。この場合オリジナルのメモリカードと完全に同じデータ列を持った別のメモリカードができる事になり、システム機器はこれらを判別することは困難である。本実施例は上記問題点を鑑みなされたもので、デッドコピー操作に対する対抗策を提示するものである。

【００７４】本実施例の主旨は、一般に公開されている情報ではアクセスできない領域、またはアクセスされたとしても自由なデータ書き換えができない領域に、メモリカードを個別に識別する識別コードを持たせ、かつファイル中にも同識別コード、または関連付けられた情報を取り込み、システム機器が両者の情報の合致を確認するという事である。

【００７５】例えば、図１に示したフラッシュメモリカードを含む不揮発性半導体メモリは一般的にＩＤリードと呼ばれる動作モードを有している。本モードはメモリの製造メーカーや、種別、容量、電気的な仕様等を外部の通知するためのモードである。例えば、図１に提示したフラッシュメモリーカードでは図１５に示すような手法によって実行される。ＩＤリードコマンド（ここでは９０ｈ）を投入すると、製造メーカーを示すコード（Maker Code）およびメモリの種別を示すデバイスコード（Device Code ）が順次出力される。例えば、株式会社東芝製の64メガビットのフラッシュメモリカードを例に取ると、１バイト目にＪＥＤＩＣ　ＩＤ９８ｈが出力され、２バイト目に６４メガビットで、動作電源３．３Ｖ品のＮＡＮＤ型フラッシュメモリであることを示すデバイスコードＥ６ｈが出力される。おなじ６４メガビットのメモリでもそれが、フラッシュメモリではなく、マスクロムであれば、Ｄ６ｈが出力される。システム機器はこれらの情報を読み取り、デバイスの仕様に適合した制御を実行する。

【００７６】本発明においては、このＩＤリード動作の動作を拡張させる。図１６に示すように本来のＩＤリード動作で必要な出力の後に、メモリカード固有の識別情報を出力するようにする。何バイト目から上記識別情報の出力が始まり、何バイト継続するのかは自由度がある。従来の製品と本機能をサポートしている製品の判別を確実に行うため、まずサポートしていること自身を提示する出力（例えばＡＡｈ等、偶然バス上にデータが存在している確率が小さいデータを設定）したのち、識別コードを出力させるようにしても良い。既に記述のごとく、本識別コードは、全てのフラッシュメモリカード１枚ずつにつき、ユニーク（固有）である必要はない（勿論固有であることが望ましい）。例えば、識別コードが１バイトで形成された場合、取りうる値としては００ｈからＦＦｈまでの２５６通りである。従ってフラッシュメモリーカードは２５６種類のグループに分類できることになる。この場合でもエンドユーザーが２人いて同一の識別コードを有するメモリカードを有している確率を考慮すると十分低いと考えられる。

【００７７】また、上記実施例では、既存のＩＤリード

コマンドを流用したが、新たに識別コードのリードコマンドを別途規定しても良い。アクセス方法が公開されているIDリードコマンドを使用するのに比べて安全性が高い。この場合の概要を図１７に示す。ここでは識別コードのリードコマンドとして１サイクルのコマンド設定を例示したが、複数バイトのコマンド入力を必要としても良い。

【００７８】また、識別コードの決定方法は種々考えられる。まずフラッシュメモリカードの製造段階で決定する方法を例示する。設定値は、例えば通し番号に様に一枚一枚をほぼ完全に識別するようしてもかまわないし、乱数を発生させて決定しても良い、ウエハ単位で決定しても良いし、チップ単位に設定しても良い。ある確率でメモリカードが他のメモリカードと異なる識別コードを持つ様に値を設定するなら、本発明の主旨に完全に合致している。メモリカードの製造メーカーで決定するのではなく、例えば著作物を記憶して販売するメーカーで決定してもかまわない。

【００７９】また、識別コードの書込み方法も種々考えられる。まずフラッシュメモリカードの製造段階で書き込む方法を例示する。例えば、図１８に示すようにヒューズを使用する方法がある。ヒューズを切ったときと、切らない時では、電源投入時に本回路が保持している値が異なる。本回路を少なくても１個以上用意しておき、設定する識別コードの値によってヒューズを切るか切らないかを決定する。例えば、識別コードのリードコマンドが投入されると、本回路に保持されている値が、出力バッファを介して外部へ出力される。ヒューズの種類としては各種想定できる。レーザーで焼き切るもの、電流を流して電気配線を熱的に焼き切るもの、ヒューズ自身がＥＥＰＲＯＭのような不揮発性メモリで構成され、電気ヒューズ等と同様の効果を発揮するもの等なんでも良い。また、チップをアッセンブリする際のボンディングオプションとしてもよい。チップ上に金配線等を接続するためのパッドを用意しておき、そのパッドを例えば、電気的にＶＣＣに接続するが、ＧＲＤに接続するかによって、保持する値が変るようにしてもかまわない。また、製造時に使用する配線層のマスクを使い分けることによっても良い。例えば、製造の最終工程に近いアルミの配線層を形成する工程でマスクを複数種類使い分ければ、ある程度のバラエティーを持っ識別コードの設定が可能である。その他小型のディップスイッチを埋め込むような形である程度機械的に設定可能なようにしても良い。また識別コードを保持した別の不揮発性メモリーを、フラッシュメモリカードとは別に持つ様にし、その別の不揮発性メモリから識別コードの値が得られるようにしてもかまわない。すなわちフラッシュメモリカード中に著作権保護のために使用する何らかのＩＣや部品をフラッシュメモリと同時に搭載するようにすれば良い。製造段階で何らかの手法により、メモリカード内に個別の識別コードが書き込まれれば良い。識別コードは電気ヒューズを切る等によって以降、書き替えが不可能なように設定しても良いし、ＥＥＰＲＯＭ等をヒューズ代わりに用いて、以降書き換えが可能な様な構造にしておいてもかまわない。この書き換えが可能な場合、必要に応じある時点以降の書き換えを不可能とするような手段、例えば電気ヒューズを切る事によって以降書き換えができなくなるようなモードを持つと汎用性が広がる。

【００８０】また、ファイル中の識別コードに関連付けられた情報とは広義である。ファイルが全体的あるいは部分的に暗号化されており、その暗号を解くカギがの識別コードそのもの、または識別コードと関係付けられたものでも良い。この場合、識別コードとファイル中の識別コードに関連づけられた情報との、合致および不一致は、正常に暗号が解ける、解けないと言い換えることが可能である。

【００８１】（第８の実施例）次に、上記第７の実施例のさらに異なる形態として、本願発明のメモリシステムの第８の実施例を説明する。本実施例は上記実施例７と異なり、フラッシュメモリ中にユーザーの使用領域とは、別のメモリ空間を準備し、そのメモリ空間上にフラッシュメモリーカードの個別の識別情報を格納することを主旨とする。

【００８２】例えば、６４メガビットのメモリの場合、ユーザーが使用可能なメモリ空間は当然６４メガビット分確保されているが、この６４メガビット分のメモリ空間とは別のメモリ空間を持ち、その中に識別情報を保持する。勿論、この冗長なメモリ空間は、６４メガビット分の正規のメモリ空間にアクセスする方法とは異なる方法によってアクセスできるようにする。

【００８３】図１９にこのフラッシュメモリの物理ブロックの概要を示す。例えば、６４メガビットのフラッシュメモリの場合、メモリセルアレイは、６４キロビット単位に１０２４のブロック（消去単位）に分割されている。この１０２４個のブロックの他に例えば８個の冗長なブロックを用意する。これらの冗長ブロックは、一般に知られているように、製造時に不良ブロックが発見された際、ブロックの置換を行う処理に用意されているブロックと兼用しても良いし、別途用意しても良い。この冗長なブロックにアクセスするための特別なコマンドを用意する（以降、冗長ブロックアクセスコマンドと呼ぶ）。本冗長ブロックには、メモリカードを個別に識別するための識別コードが書き込まれる。実施例７で説明したように識別コードをどの段階で書き込むかは自由度を持つ。例えば製造段階で本領域に識別コードが書き込まれたとし、そのメモリカードに著作物を格納して販売をするケースを考えると、著作物を書き込む際、書込みツールは、冗長ブロックアクセスコマンドにより、冗長ブロックに書き込まれた識別コードを読み取る。次に、この読み取った識別コードまたは識別コードに関連付け

られた情報をファイル中に取り込み、メモリカードにファイルを書き込む。システム機器は冗長ブロックに書き込まれたメモリカードの識別コードとファイル中に取り込まれたメモリカードの識別情報を比較し、所定の条件を満たした場合にシステム機器上での使用を許可する。ファイルがあるメモリカードから別のメモリカードへハードディスク等を介して転送され、別のシステム機器上で動作させようとしても、コピーファイルの転送先のメモリカード中の冗長ブロックに書き込まれた識別コードと、コピーされたファイルに取り込まれたメモリカードの識別情報が合致しないので、使用できない。これによって著作物の権利が保護されることになる。

【００８４】この冗長ブロックへ書き込まれるメモリカードの識別情報の形態は、これまでの実施例の中で述べてきたように種々考えられる。メモリカードの識別コードを単純に格納してもよいし、複数個格納して実際に使用する際、比較して使用してもよい。また、識別コードの妥当性を判断するための付加的な情報を付けてもよい。例えば、パリティを計算しその計算結果と共に格納したり、エラー訂正用の符号とともに格納しエラーが発生した場合、エラー訂正が可能としてもよい。また識別コードをその補数（例えば識別コードがＡＡｈならその補数として５５ｈ）と共に格納するようにしてもよい。また、図１のメモリカードで実際のファイルを格納する際使用しているＥＣＣの方式がそのまま適用可能なようにしてもよい。また図１に例示したフラッシュメモリで例えば１ブロックが１６ページで構成されているならば、複数のページに識別コードを格納しても良い。また、複数個のブロックに格納されてもかまわない。また識別コードのほかに、その冗長ブロックが識別コードを格納していることを確認するための情報（例えば規定された１文字以上の文字列等）や、該当する冗長ブロックが電気的に正常なものか不良ブロックかを示すフラグのような管理データと共に格納されてもよい。例えば、識別コードを格納するための領域として２ブロック分（優先度は設けても良い）を用意しておけば、仮にその一つが不良のブロックとなっている場合でも、製造歩留まりを落とさずにすむ。この場合システム機器としては、まず管理フラグをみて、正常なブロックか否かを判断し、次に識別コードが格納されているかどうかを規定の文字列の有無で判断する。規定の文字列が見つかったら、識別コード妥当性をパリティその他の手段を使って判断しながら、識別コードを取得する。もし最初にアクセスしたブロックが不良ブロックであったら、次のブロックにアクセスに行くのは自明である。その他さまざまな方法が考えられるが、実施例７で記述した通り、ユーザーが簡単にアクセスできない領域に、メモリカード個別の識別情報が格納されれば本発明の主旨に合致する。

【００８５】また、ファイル中の識別コードに関連付けられた情報とは広義である。ファイルが全体的あるいは部分的に暗号化されており、その暗号を解くカギが識別コードそのもの、または識別コードと関係付けられたものでも良い。この場合、識別コードとファイル中の識別コードに関連づけられた情報との、合致および不一致は、正常に暗号が解ける、解けないと言い換えることが可能である。

【００８６】（第９の実施例）次に、上述した第８の実施例をさらに強化した形態の本願発明のメモリシステムの第９の実施例を説明する。実施例８では、識別コードの書き換えを禁止する方法を明示していないので、万が一、冗長ブロックへのアクセス方法が流出した場合、該当領域のデータを書き替える不正なツールが作られないとも限らない。本実施例は実施例８で開示した方法にさらに、識別コードの書き換えを禁止する措置を付加したものである。

【００８７】図１９を用いて具体的な例を説明する。例えば６４メガビットのフラッシュメモリの場合、メモリセルアレイは、６４キロビット単位に１０２４のブロック（消去単位）に分割されている。この１０２４個のブロックの他に例えば８個の冗長なブロックを用意する。ここで示したブロックの各々には図２０に示すようなロウデコーダがついている。このロウデコーダの機能について説明を加える。

【００８８】ロウデコーダ回路は、チップに入力されるアドレスに従いブロックを選択し、ワード線等に周辺回路中にて発生した電圧を転送する役割を担う。通常は、データ書込み・データ消去・データ読出しの全てにおいて上記動作を行う。以下に、図２０に従い、ロウデコーダ回路の動作を説明する。

【００８９】信号ＲＤＥＣはロウデコーダの起動信号であり、書込み・消去・読出しの動作時には“Ｈ”となる。信号ＡＤＤＲＥＳＳはブロックアドレスを表す信号であり、アドレスが選択されたブロックのみ複数のアドレス信号が全て“Ｈ”となり、ノードＮＡも“Ｈ”となる。書込み動作時及び読出し動作時には、信号ＥＲＡＳＥが“Ｌ”、信号／ＥＲＡＳＥが“Ｈ”となり、「信号経路１」を介してノードＮＯに信号が伝わる、つまり選択されたブロックではノードＮＯが“Ｈ”、それ以外のブロックでは“Ｌ”となる。すると、選択ブロックでは、ノードＮ１＝ＶＰＰ（書込み・消去・読出し等を実現するための高電圧）、／Ｎ１＝０Ｖとなり、周辺回路部バスラインの電圧がワード線に伝わり（図の右下の破線内回路参照）、データの書込み・読出しが実行される。また、非選択ブロックでは、Ｎ１＝０Ｖ、／Ｎ１＝ＶＰＰとなり、周辺回路部バスラインとワード線が非接続状態にある。

【００９０】次に、消去動作中の詳細な動作について以下に説明する。消去動作開始前には、信号ＲＥＳＥＴが“Ｈ”の状態にあるため、ノードＮＬ、ＮＲはそれぞれ“Ｈ”、“Ｌ”のレベルにある。消去動作が開始する

と、信号ＲＥＳＥＴが“Ｌ”となり、またチップに入力されたアドレスに従ってアドレス信号ＡＤＤＲＥＳＳが設定され、さらに信号ＬＥＳＴがある一定時間“Ｈ”となる。選択ブロックでは、ノードＮＡが“Ｈ”にあるため、ＦＵＳＥが非切断状態にある場合には、ＦＵＳＥを介してノードＮＬが０Ｖと接続されるため、ノードＮＬ、ＮＲがそれぞれ“Ｌ”、“Ｈ”となる。一方、ＦＵＳＥが切断状態にあるブロックでは、ブロックの選択・非選択に依らず、ノードＮＬ、ＮＲはそれぞれ“Ｈ”、“Ｌ”の状態が保たれる。続いて、信号ＥＲＡＳＥが“Ｈ”、信号／ＥＲＡＳＥが“Ｌ”となり、「信号経路１」を介してノードＮＯに信号が伝わる、つまりノードＮＲの電圧がＮＯに伝わり、ノードＮＲが“Ｈ”レベルにあるブロックに対してのみデータ消去が実行される。

【００９１】以上述べたことから明らかなように、図２０中のロウデコーダ回路では、データ書込み・読出し時のブロックの選択／非選択は直接アドレス信号を用いて行い、一方データ消去時のブロックの選択／非選択は回路中のラッチ回路を用いて行う。従って、図２０中の回路を用いることにより、ＦＵＳＥが切断されたブロックでは、データの書込み・読出しは実行可能、データ消去は実行不可能とすることができる。

【００９２】上記ロウデコーダを使用した場合、下記の様に制御を行う。例えば冗長ブロックにアクセスするコマンドを用意する。本領域にメモリカードに固有の識別コードを書き込む。識別コードの書込みフォーマットに関しては様々な方法が想定可能な事は、既に実施例８等に記載してある。本実施例では、識別コードを書き込んだ後、ＦＵＳＥを切断する。ヒューズの種類がレーザーカットのもの、電気ヒューズ、ＥＥＰＲＯＭ等取りうることは記述である。ＦＵＳＥを切断すると記述のように、書込み・読み出しは可能となるが、消去動作は禁止される。従って該当領域へのアクセス方法が仮に流出したとしても、該当領域に格納された情報を自由に書き替えることはできない。ただし、この実施例では、書込み動作は禁止をしていない。従って追加の書込み動作は可能である。本実施例中のフラッシュメモリは消去動作なしで“１”のデータを“０”に書き替えることは可能であるが、“０”のデータを“１”に書き替えることはできない。従って、メモリカードの識別情報を格納する際、識別コードのほかにその補数を同時書き込んでおけば良い。例えば識別情報が、“ＡＡｈ＝１０１０１０１０”とするとその補数は“５５ｈ＝０１０１０１０１”となる。不正な操作により、識別コードのＡＡｈの最上位のビットを追加書込みして“２Ａｈ＝００１０１０１０”に書き替えたとしても、対応する補数格納領域を“Ｄ５ｈ＝１１０１０１０１”に書き替えることはできない。従って識別コードを補数と共に格納することにより、不正な追加書込みが不可能となり、たとえ該当領域へのアクセス方法および追加書込み方法が分かったとしても該当領域に対し意味あるデータの書き換え行為ができないことになる。従って本領域にメモリカードを個別に識別する識別コードが書かれ、識別コードまたは関連付けられた情報がファイル中に取り込まれ、両情報の比較によってシステム上での動作を制限する仕組みのシステム機器においては、仮にファイルを別のメモリカードにコピーしたとしても、転送先のメモリカードにも同様に識別情報の格納領域があり、その情報の書き換えも同様に制限されているので、その識別情報とファイル中の情報の合致がなくシステム機器上で使用できず、著作物の権利が保護されている。メモリカードの出荷後、著作物を格納するメーカーの時点で同領域に情報を書き込む場合は、識別情報格納後、例えば電気ヒューズであれば電気的にヒューズを切断して以降の不正な識別情報の書き換えを禁止する。ここでは消去動作のみを禁止したが、同様の手段よって該当領域の書込み動作自身を禁止しても良い。消去および書き込みを禁止する手段としてはロウデコーダ近辺のヒューズのみに限られない、該当領域にアクセスが有った場合、書込みおよび消去に必要な高電圧の発生回路の動作を禁止するような手段をとっても良いし、任意である。識別情報を格納した後、何らかの手段によって、該当領域の消去動作または、書き込み動作のいずれか一方もしくは両方の動作が禁止されれば本発明の主旨を満足する。一旦禁止された消去または書き込み動作が、更に複雑な手順を経て再び消去および書込み動作が可能となるような方法を保持しておいてもかまわない。

【００９３】上記実施例では、メモリカードの識別コードは冗長ブロックに格納したが、本発明はこれに限られない。冗長ブロック以外の通常のメモリ空間領域に格納してもかまわない。図１に示したメモリカードでは記述のようにブロック単位でブロックの不良登録が可能である。あるブロックを識別コードの格納ブロックと定義してそこに識別コードを書き込んだ後、ヒューズと切断する等の手段により不正な識別コードの書き換えを防ぐようにしても良い。この時通常のシステムが該当ブロックを通常のデータ格納領域として使用しようと試みるのを防ぐため、識別コードに関連する情報を格納するほか、ブロックのＢｌｏｃｋ　ＳｔａｔｕｓＡｒｅａにマークをつけ不良ブロック登録しておけば良い。記述のようにこれらのケースの場合も識別コードを格納していることが確認できるような情報を一緒に格納しておけば良い。この方法を使用する場合は、あるメモリカードののデータが、他のメディアにデッドコピーされてはいけないので、全てのメモリカードの出荷時に識別コードを書き込み、フューズを切断して以降の消去動作もしくは書込み動作の一方もしくは両方の動作を禁止するようにすれば良い。従って通常のメモリ空間に識別コードを記憶し、該当領域に対し、以降の消去動作もしくは書込み動作の一方もしくは両方の動作を禁止するような手段を持って

いれば本発明の主旨を満足する。また、上記実施例の１から９中では説明を簡略化するために単にメモリカードの識別番号と記載しているが、それが単純にメモリカードの識別番号だけではなく、著作物を直接識別するための情報（例えば音楽ファイルの場合、販売者や歌手、作曲家、作詞家、製造者、レコードメーカー、アルバム名、局名等メモリカード自身の固有性と直接関係なくてもよい）であってもかまわない。

【００９４】また、ファイル中の識別コードに関連付けられた情報とは広義である。ファイルが全体的あるいは部分的に暗号化されており、その暗号を解くカギが識別コードそのもの、または識別コードと関係付けられたものでも良い。この場合、識別コードとファイル中の識別コードに関連づけられた情報との、合致および不一致は、正常に暗号が解ける、解けないと言い換えることが可能である。

【００９５】（第１０の実施例）次に、本願発明のメモリシステムの第１０の実施例を説明する。本実施例はデータをデッドコピーするようなツールに対する防御機能に関するものである。

【００９６】ここではメモリの内部にランダムに適当な頻度で不良ビットを持たせる。この時、記憶媒体である不揮発性メモリの内容を複製しようと、元のメモリカードからデータを読み出して複製先のメモリカードにデッドコピーを行おうとしても、書き込み先のメモリに存在する不良ビットの存在によりその部分に正しくデータを書き込めず、正しくコピーすることは出来ず不正なデータコピーは失敗に終わる。上記の不良ビットは先天性の不良ビットでも人為的に配置された不良ビットでも同様の効果が期待できる。また、さらに、不良はビットである必要はなく、ビットの他にロー不良、カラム不良、ブロック不良、及びそれらの組み合わせを先天的に若しくは人為的に持つ不揮発性メモリでも同様の効果を期待できる。

【００９７】不良ビット、ロー、カラム、またはブロックを人為的に生じせしめる手段としては、レーザー照射によるセルトランジスタ、ローデコーダ、カラムデコーダ、若しくはブロックデコーダの破壊が考えられる。また、同様にポリシリコンヒューズまたは電気ヒューズをセル、ロー、カラム若しくはブロックとそれらのデコーダとの間に設け、それをレーザまた過電流で溶断する手法も考えられる。さらにはＯｎｅ　Ｔｉｍｅ　ＰＲＯＭ等の不揮発性メモリのセルを設けそのセルに書き込みを行う事により人為的に上記の不良の中の一つまたはそれらの組み合わせを作る等、本発明の趣旨を逸脱しない範囲で人為的に不良を作ることは可能である。実施例８または９で説明したような手法により消去動作または書込み動作の一方または両動作を禁止してもよい。消去動作のみを禁止する場合、あらかじめ該当領域に“０”データを書き込んでおけば、データのコピーができないので同様の効果が出る。データのデッドコピーを実行しようとした際、なんらかの方法により、コピーが失敗するような対策が施されていれば本実施例の主旨に合致することになる。

【００９８】（第１１の実施例）次に、本願発明のメモリシステムの第１１の実施例を説明する。上記１から１０の実施例において著作物の権利保護の仕組みについて説明したが、著作物の権利保護機能を有するメモリカードとそうでないカードの判別が可能なようにしても良い。判別の方法は種々考えられる。例えばメモリカードの外装表面に著作権保護機能がついていることを表す文章や、ロゴマークがついていても良い。また色や模様の規定を行い、それが著作権保護機能を持っているという事にしても良い。また製品名や製品型番から分かるようにしても良い。またシステム機器の挿入された場合、例えばディスプレイ上にメッセージが出るようにしても良い。またＰＣ上でファイルを取り扱う際、メッセージ等が出るような仕組みでも良い。またシステム機器内のコントローラに相当する部分が判別可能なように、既に記述したが、ある特定の操作（例えば著作権保護機能がついているかどうかを出力する特殊なコマンド等）によって判別できれば良い。

【００９９】また、上記のような著作権の保護がされているかどうかをファイル単位またはディレクトリ単位で判別可能なようにしてもよい。また、私的に作成された音楽や、プロモーション用の音楽等の著作物で保護の必要のないものを想定し、著作権保護の必要の無いものなのか、または不正にコピー等をされたものなのかを判別できるようにしても良い。ファイル中の所定の領域に例えばフラグを設けて、著作権保護の必要のないものと判断されれば、これまで記載してきたような著作権保護に関する条件が成立しなくてもシステム機器上で使用可能なようにしてもよい。

【０１００】上記１から１１実施例において、フラッシュメモリカードを例に説明したが、本発明はフラッシュメモリカード、さらには半導体メモリのみに限られない。カードの全体がマスクＲＯＭ（ＭＲＯＭ）で構成されていても良いし（この場合、上述の実施例１から１１で説明した識別コード等もＭＲＯＭ化されていても良い）、ＭＲＯＭと共に上述の実施例１から１１で説明したような機能を盛り込むためにデータ書込みや識別コードの設定が可能なフラッシュメモリや、ＯＴＰ（Ｏｎｅ　Ｔｉｍｅ　ＰＲＯＭ）やヒューズ等が付随していてもかまわない。

【０１０１】さらに、本発明は上記実施例に限られものでなく、主旨を逸脱しない範囲で種々変更して利用可能である。また、これらの著作物の権利保護が上記実施例１から１１単独もしくは組み合わせたもののみで使用されなくてもかまわない。例えば、電子透かし技術や、暗号化技術と共に使用されても良い。

【０１０２】

【発明の効果】本願発明は、メモリカードを個別に識別する情報を保持する領域をメモリカード上に設け、この情報をもとにメモリカードに記憶されるデータを読み出す種々の方法を提供することで、メモリカード上のファイルに対し著作権保護を目的としたコピーガードの機能を附加するものである。

【図面の簡単な説明】

【図１】フラッシュメモリカードの外観を示す図である。

【図２】１６MビットＮＡＮＤ型フラッシュメモリの物理ブロックの構成を示す図である。

【図３】１６MビットＮＡＮＤ型フラッシュメモリのデータ領域内部の構成を示す図である。

【図４】１６MビットＮＡＮＤ型フラッシュメモリの論理ブロック／物理ブロック変換テーブルの構成を示す図である。

【図５】１６MビットＮＡＮＤ型フラッシュメモリの物理ブロックの構成を示す図である。

【図６】１６MビットＮＡＮＤ型フラッシュメモリの物理ブロックの構成を示す図である。

【図７】図５および図６に示すＣＩＳ領域の構成を示す図である。

【図８】本願発明の第１の実施例の概要を示す図である。

【図９】本願発明の第２の実施例の概要を示す図である。

＊【図１０】本願発明の第２の実施例の概要を示す図である。

【図１１】本願発明の第４の実施例の概要を示す図である。

【図１２】本願発明の第４の実施例の概要を示す図である。

【図１３】本願発明の第４の実施例の概要を示す図である。

【図１４】本願発明の第５の実施例の概要を示す図である。

【図１５】従来のフラッシュメモリカードのＩＤリードモード時の各信号波形を示した図である。

【図１６】本願発明の第７の実施例に係るフラッシュメモリカードのＩＤリードモード時の各信号波形を示した図である。

【図１７】本願発明の第７の実施例に係るフラッシュメモリカードのＩＤリードモード時の各信号波形を示した図である。

【図１８】フラッシュメモリカードに搭載されるフューズ回路の一例を示す回路図である。

【図１９】本願発明の第８の実施例に係るフラッシュメモリカードの物理ブロックの構成を示す図である。

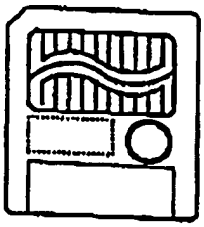
【図２０】本願発明に係るフラッシュメモリのロウデコーダ回路の一例を示す図である。

【符号の説明】

ＦＵＳＥ　　ヒューズ

＊

【図１】



【図２】

		0 … 255	256 … 263
Block 0	Page 0	データ領域(256バイト)	冗長部(8バイト)
	Page 1		
	：		
	Page15		
Block 1	Page 0		
	Page 1		
	：		
	Page15		
：	：	：	：
Block 511	Page 0		
	Page 1		
	：		
	Page15		

【図６】

Block 0	不良ブロック
Block 1	CIS
Block 2	Data
：	：
Block 511	Data

【図3】

◎データ部

バイト	0ページ（偶数ページ）	1ページ（奇数ページ）
0 ～ 255	DATA Area-1.	DATA Area-2

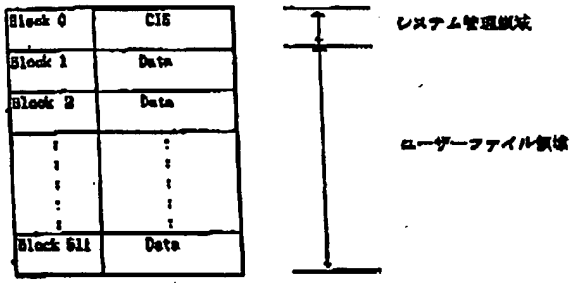
◎冗長部

バイト	偶数ページ	奇数ページ
256	Reserved Area	ECC Area-2
257	Reserved Area	
258	Reserved Area	Block Address Area-2
259	Reserved Area	
260	Data Status Area	
261	Block Status Area	ECC Area-1
262	Block Address Area-1	
263		

【図4】

OFFSET	Upper Byte	Lower Byte
Word0 (LBA=0)	Physical Block Address上位	Physical Block Address下位
Word1 (LBA=1)	Physical Block Address上位	Physical Block Address下位
Word2 (LBA=2)	Physical Block Address上位	Physical Block Address下位
Word498 (LBA=497)	Physical Block Address上位	Physical Block Address下位
Word499 (LBA=998)	Physical Block Address上位	Physical Block Address下位
Word000 (LBA=999)	Physical Block Address上位	Physical Block Address下位

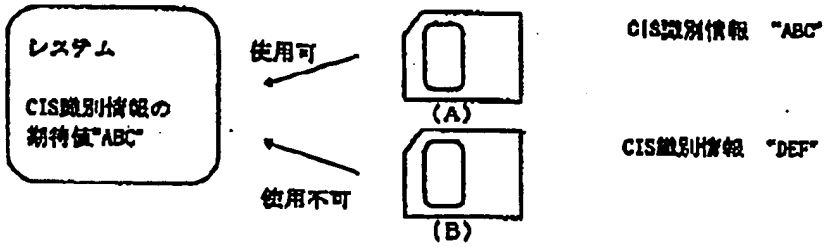
【図5】



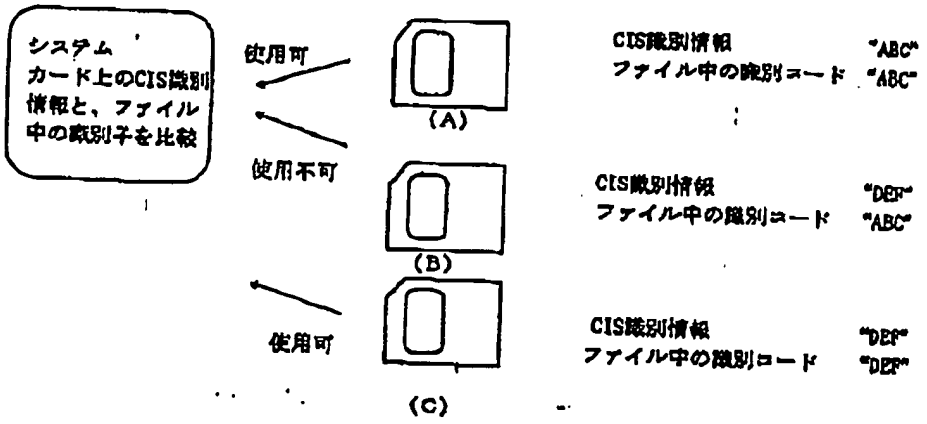
【図7】

領域A	固定データ領域。先頭10バイトで標準フォーマットへの準拠の有無を判断する。
領域B	任意のデータが設定可能な領域。

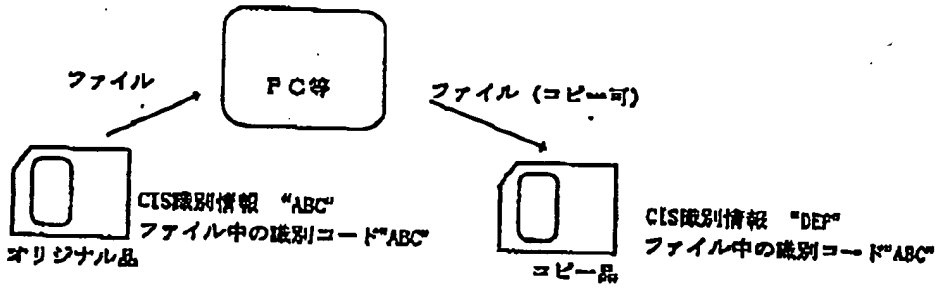
【図8】



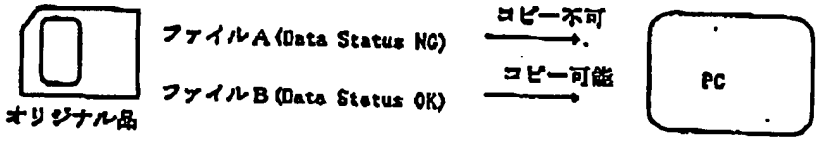
【図９】



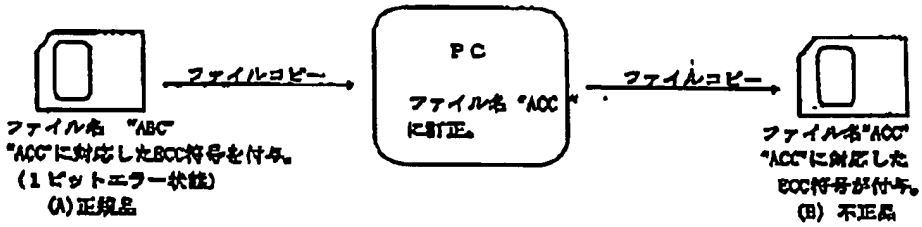
【図１０】



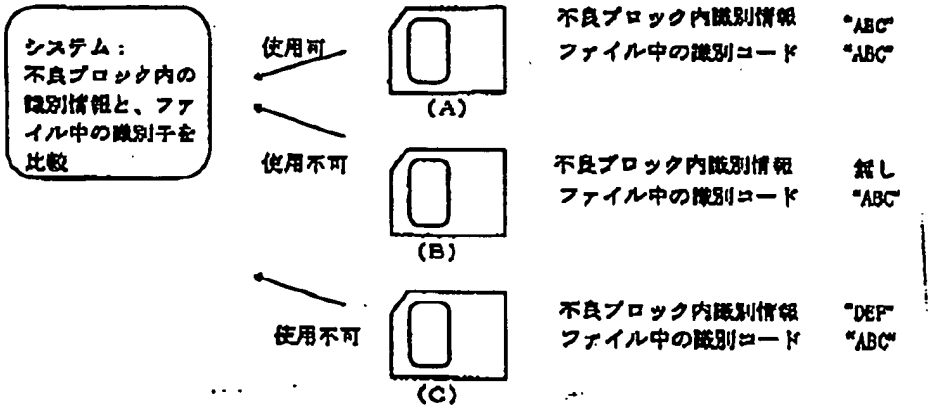
【図１１】



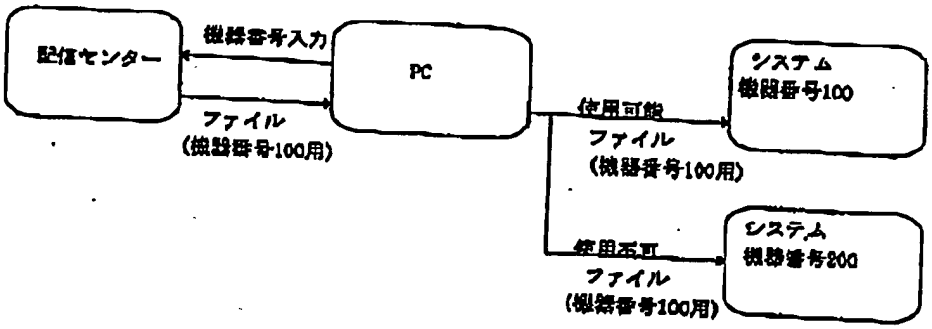
【図１３】



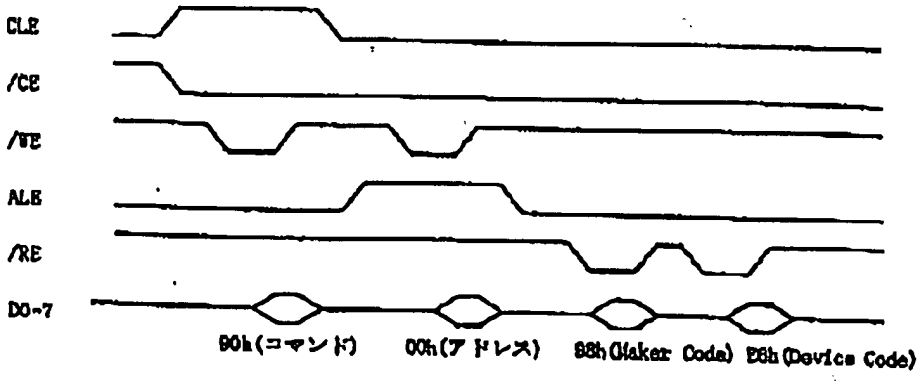
【図12】


システム：
不良ブロック内の識別情報と、ファイル中の識別子を比較
使用可
使用不可
使用不可
(A)
(B)
(C)
不良ブロック内識別情報　"ABC"
ファイル中の識別コード　"ABC"
不良ブロック内識別情報　無し
ファイル中の識別コード　"ABC"
不良ブロック内識別情報　"DEF"
ファイル中の識別コード　"ABC"

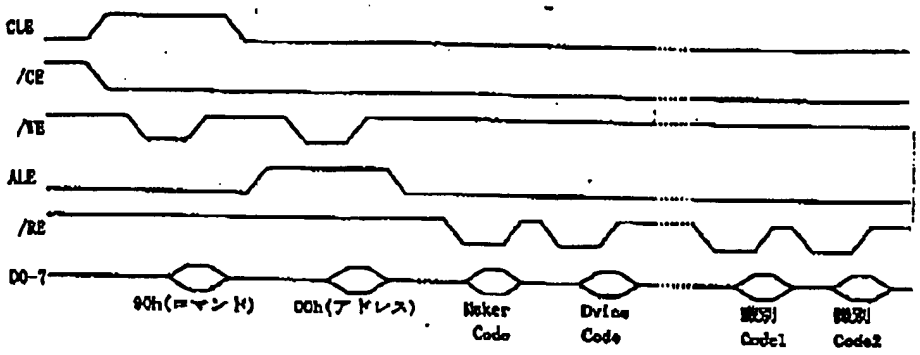
【図14】


配信センター
機器番号入力
ファイル
(機器番号100用)
PC
使用可能
ファイル
(機器番号100用)
システム
機器番号100
使用不可
ファイル
(機器番号100用)
システム
機器番号200

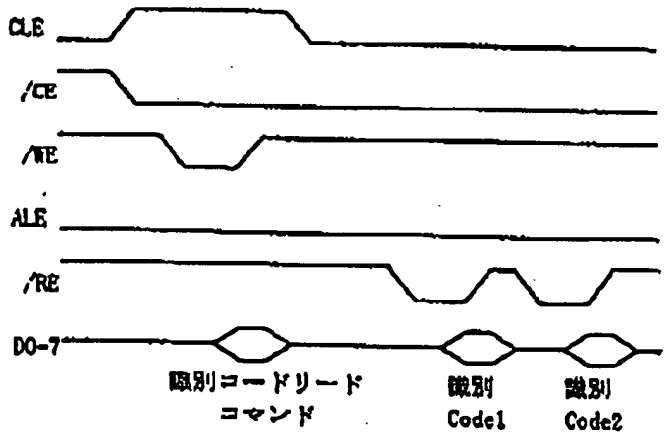
【図15】


CLE
/CE
/WE
ALE
/RE
D0-7
90h(コマンド)
00h(アドレス)
98h(Maker Code)
D6h(Device Code)

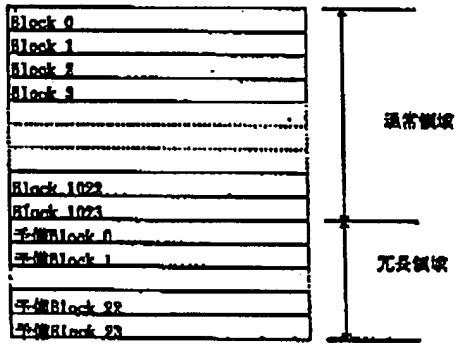
【図16】



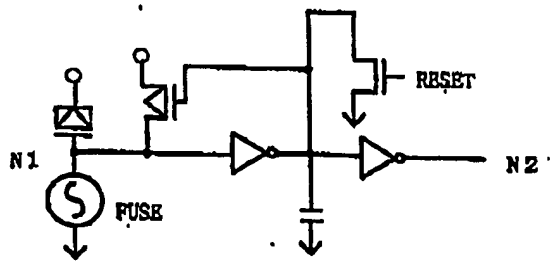
【図17】



【図19】

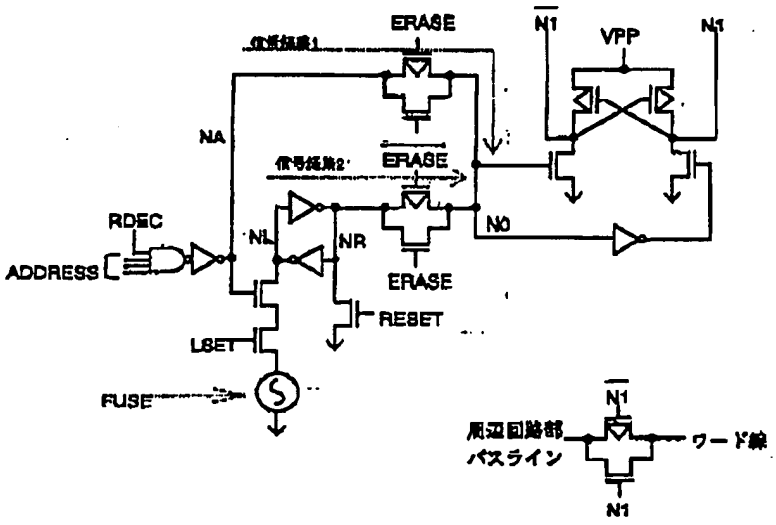


【図18】



FUSE	N1	N2
切る	"H"	"H"
切らない	"L"	"L"

【図20】



フロントページの続き

(72)発明者　中林　幹戸
神奈川県川崎市幸区堀川町580番1号　株式会社東芝半導体システム技術センター内

(72)発明者　中村　寛
神奈川県川崎市幸区堀川町580番1号　株式会社東芝半導体システム技術センター内

Fターム(参考)　5B017 AA06 AA07 BA04 BA05 BA07
BB08 CA11 CA12 CA14 CA16
5B025 AE10
5B060 AB26 AC12 MM09 MM12 MM16